POLITECNICO DI TORINO

Corso di Laurea Magistrale in Ingegneria Gestionale

ASPETTI ECONOMICI REGOLATORI DEL CLOUD COMPUTING E DELLA CYBERSECURITY

Relatore

Professore Carlo Cambini

Candidato

Maria Elena Cuccia

Anno Accademico 2023/2024

Indice

Ringrazio il mio relatore Carlo Cambini per i suoi preziosi consigli, la disponibilità e la gentilezza dimostratami durante quest'ultima fase del mio percorso di studi, concedendomi la possibilità di raggiungere questo traguardo.

Ringrazio la mia famiglia per avermi sempre sostenuta ed incoraggiata,

in particolare mio fratello Vincenzo per essere da sempre la mia guida.

Ringrazio Alessandro per essere stato sempre al mio fianco.

ABSTRACT

Nell'ultimo decennio abbiamo assistito ad un cambiamento fondamentale nel modo in cui le aziende accedono alle tecnologie digitali. Tradizionalmente, ciò richiedeva alle aziende di effettuare notevoli investimenti iniziali in infrastrutture hardware e software e di mantenere grandi reparti IT. Adesso, in alternativa, le aziende acquisiscono le proprie esigenze di storage, elaborazione e software come servizio, pay as you go, attraverso quello che viene comunemente definito "cloud computing". In particolare, il cloud computing è il pilastro per quanto riguarda l'archiviazione e la gestione dei dati che nel panorama digitale odierno rappresentano l'asset strategico più importante per le organizzazioni tanto che il successo o il fallimento di un'organizzazione dipende dalla sua capacità di raccogliere, elaborare e utilizzare in maniera efficiente queste informazioni che gli permettono di segmentare il mercato ed estrarre più surplus dai consumatori. Allo stesso ciò introduce nuove sfide legate alla protezione dei dati e la fiducia nella sicurezza diventa fondamentale per l'adozione del cloud, poiché le aziende e gli individui affidano ai provider di servizi cloud le proprie applicazioni critiche. Pertanto, il cloud computing e la cybersecurity sono due facce della stessa medaglia. Questo lavoro di tesi si propone di studiare attraverso un modello di Hotelling, la competizione tra due cloud service providers con quote iniziali di mercato diverse, in presenza costi di switching ed investimenti in sicurezza. I clienti, massimizzando la loro utilità, decidono se rimanere con il provider scelto oppure cambiare fornitore sostenendo un costo di switching legato a diversi fattori quali la necessità di spostare i dati, la perdita di economie di apprendimento ed eventuali incompatibilità tra sistemi diversi.

CAPITOLO 1 – LETTERATURA

1.1 STORIA DELL'EVOLUZIONE DEL CLOUD COMPUTING

Ripercorriamo la sua evoluzione, dagli albori delle reti informatiche fino alla sua adozione su larga scala nel mondo moderno. Una figura fondamentale per la nascita del cloud computing è stata l'informatico statunitense John McCarthy, che possiamo considerare l'antesignano dell'intelligenza artificiale. McCarthy nel 1960 propose per la prima volta l'idea che l'elaborazione dei dati potesse essere organizzata come un *servizio pubblico*, simile alle utility come l'elettricità o l'acqua. Questa visione precoce prefigurava la capacità di fornire risorse computazionali a più utenti da un'infrastruttura centrale. Nel 1966, Douglas Parkhill descrisse, nel suo libro "*The Challenge of the Computer Utility*" diverse caratteristiche come l'elasticità, la virtualizzazione e il pagamento a consumo, caratteristiche riconducibili al cloud computing moderno. Il concetto di "utilità informatica" inizia a concretizzarsi, gettando le basi per ciò che diventerà il cloud computing. Nel 1969 si assiste allo sviluppo di Arpanet (Advanced Research Projects Agency Network) grazie al lavoro di JCR Licklider, che ha creato per scopi militari su commissione dal Dipartimento della Difesa degli Stati Uniti la prima rete di comunicazione elettronica, che consentiva di effettuare uno scambio di informazioni in maniera rapida, sicura e proficua, grazie ad Arpanet furono poste le fondamenta per la condivisione di risorse a distanza tra computer. Nasce così il grid computing, antenato del cloud computing. Questa visione di JCR Licklider che possiamo considerare rivoluzionaria per quel periodo, pose le basi per uno sviluppo inarrestabile del cloud computing che raggiunse il suo apice negli anni 80-90, consentendo ad ogni utente senza limiti di tempo, di interfacciarsi da ogni parte del mondo con i servizi erogati. Il lavoro di McCarthy così come quello di Licklider è stato pertanto fondamentale per un radicale cambiamento nel campo dell'informatica dell'epoca. Si fanno risalire all'anno 1979 le origini dell'e-commerce. In particolare con Compuserve nasceva il primo Internet Service Provider che offriva connessioni dial-up agli utenti, che hanno potuto sperimentare così l'accesso da remoto ai dati e ai servizi. Nel 1984, negli Stati Uniti, il fornitore di servizi Internet Prodigy introdusse una importante innovazione nel settore IT, i propri utenti potevano fruire per la prima volta di servizi specifici come forum di discussione, e-mail, servizi bancari e una piattaforma di e-commerce. Ciò costituì un passo significativo verso la commercializzazione di Internet e l'accesso a servizi online centralizzati. Il 1991 costituisce l'anno di svolta, il CERN in Svizzera rilasciò

il World Wide Web per uso pubblico, dando inizio a una delle più importanti rivoluzioni nel campo dell'informazione tecnologica dell'epoca moderna, infatti laboratori e università di tutto il mondo poterono accedere a una vasta rete di risorse e dati condivisi. L'infrastruttura web si sviluppò rapidamente, diventando la piattaforma principale per l'accesso ai servizi di cloud in futuro. Nel 1997, il professore Ramnath Chellappa dell'Università di Harvard coniò per la prima volta il termine "cloud computing". Questo concetto rappresentava la fornitura di potenza di calcolo e risorse via Internet, preannunciando la direzione che avrebbero preso le tecnologie IT negli anni successivi. La società VMware è stata una delle prime aziende a sviluppare software di virtualizzazione, che permette di eseguire più sistemi operativi su un unico computer fisico. La virtualizzazione è un elemento fondante del cloud computing, in quanto consente l'uso più efficiente delle risorse di calcolo. Quando i personal computer sono divenuti più accessibili e tutti avevano la possibilità di connettersi, Salesforce è stata la prima società globale a fornire applicazioni in rete in modalità cloud lanciando il Software as a Service alle imprese, questo modello innovativo consentiva alle aziende di utilizzare applicazioni software tramite Internet, senza doverle installare sui propri server o computer. Nel 2004, Google promosse un progetto ambizioso ed innovativo nell'ambito del panorama informativo tecnologico attraverso la creazione di diversi servizi tra cui Gmail, che rappresenta uno dei servizi di posta elettronica fondati su cloud più popolari al mondo. Gmail fu uno dei primi modelli di utilizzo del cloud per applicazioni consumer su larga scala. Nel 2006, il progetto innovativo di Google continuò con il lancio dei Google Apps, un insieme di applicazioni che funzionavano direttamente dal browser, iniziando a competere con programmi tradizionali come Word ed Excel. Contemporaneamente, Amazon promosse Amazon Web Services (AWS), una suite di servizi cloud che includeva soluzioni di Infrastructure as a Service (IaaS) e Platform as a Service (PaaS). Questo rappresentò un punto di riferimento nell'adozione del cloud computing su scala globale. Nel 2008 con la creazione di Eucalyptus, un software open source, è stato introdotto il concetto di cloud privato, permettendo alle aziende di realizzare infrastrutture cloud su server interni anziché affidarsi a fornitori esterni. Nel 2011, Apple iniziò a far parte del mondo del cloud computing attraverso la fornitura del servizio iCloud, che permetteva agli utenti di memorizzare file e dati online e di sincronizzarli tra dispositivi. Nel 2015, il numero di fruitori di Internet nel mondo ha superato i 3,3 miliardi. Questo aumento esponenziale nell'utilizzo di Internet ha condotto al crescente uso di servizi cloud da parte di persone e società in tutto il mondo. Nel 2017, le aziende

di tutto il mondo iniziarono ad effettuare notevoli investimenti oltre 5 milioni di dollari l'anno per i servizi cloud di Amazon, sottolineando quanto il cloud computing fosse divenuto una parte integrante e fondamentale delle strategie IT aziendali.

1.2 DEFINIZIONE

Secondo il NIST: "il cloud computing è un modello che consente l'accesso on demand e su richiesta, attraverso la rete, a un insieme condiviso di risorse informatiche configurabili (come reti, server, storage, applicazioni e servizi) che possono essere rapidamente fornite e rilasciate con il minimo sforzo di gestione o interazione con il fornitore di servizi."

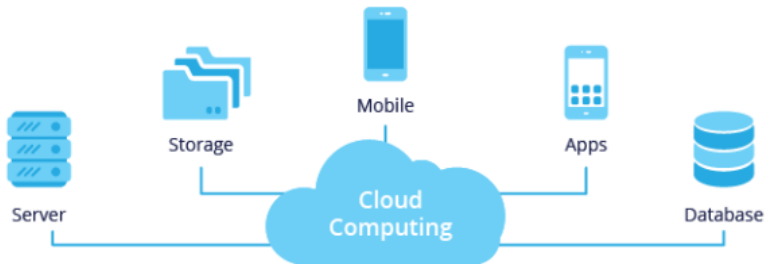

Figura 1: Cloud Computing

La definizione del NIST mette in evidenza le caratteristiche principali del cloud computing, parlando di un servizio on-demand, con tariffazione basata sul consumo, ciò permette a qualsiasi azienda di ottenere il servizio richiesto senza la necessità di dover acquistare, gestire e manutenere l'infrastruttura fisica. Si parla di democratizzazione dell'informatica (Bloom e Pierri 2018), poiché adesso "qualsiasi azienda può utilizzare (quasi) qualsiasi servizio di cui ha bisogno, quali capacità di calcolo, archiviazione e database, sulla base delle proprie necessità affidandosi a un fornitore cloud, senza la necessità di sostenere investimenti ed in qualsiasi momento."

Un esempio di tutto ciò è fornito dal caso **Instagram**.

Il caso di studio di Instagram illustra come una startup abbia sfruttato con successo il cloud computing per gestire una crescita esplosiva degli utenti. Instagram nasce nell'ottobre 2010, raggiunge 25.000 utenti nel primo giorno e 1 milione di utenti in tre mesi, 10 milioni poco dopo e

quasi 30 milioni di utenti in un anno e mezzo. Risulta evidente come una condizione necessaria, ma non sufficiente, per il successo di Instagram sia stata la sua capacità di scalare rapidamente seguendo la crescita dei suoi utenti. Tutto ciò è stato possibile grazie alle risorse del cloud computing, che hanno permesso ai fondatori di Instagram, con un budget limitato, di basare la loro applicazione interamente su un cloud pubblico, evitando la necessità di acquistare hardware fisico, molto costoso e meno scalabile.

Oltre al caso di studio di Instagram ci sono altri esempi di come le aziende e le organizzazioni hanno adottato il cloud computing per raggiungere i loro obiettivi aziendali, come Netflix, National Oceanic and Atmospheric Administration (NOAA) e la campagna presidenziale di Obama del 2012. Netflix, azienda leader nel settore dello streaming video, ha migrato la sua infrastruttura al cloud AWS, abbandonando i suoi data center fisici dopo aver subito un down service di 3 giorni consecutivi a causa di un danno al loro database. Il passaggio al cloud da parte di Netflix ha portato diversi vantaggi, gli ha consentito di aumentare la sua base di utenti di otto volte dal 2008, la visione complessiva degli utenti è cresciuta di tre ordini di grandezza questo grazie alla possibilità di scalare rapidamente e gestire le richieste di picco.

Figura 2: Netflix streaming Hours

L'agenzia federale americana ha migrato la sua soluzione di posta elettronica a Gmail di Google nel 2012, riducendo i costi della metà e semplificando la gestione degli aggiornamenti software e hardware per i suoi 25.000 dipendenti. La campagna Obama ha utilizzato in larga misura le soluzioni di cloud computing per creare un'infrastruttura IT agile e scalabile. L'utilizzo di un mix di servizi SaaS, PaaS e IaaS ha permesso alla campagna di gestire un volume elevato di transazioni online, di scalare rapidamente le sue applicazioni per gestire i picchi di traffico e di ridurre i costi complessivi.

1.3 CARATTERISTICHE ESSENZIALI

Il National Institute of Standard & Technology (NIST) definisce le seguenti caratteristiche essenziali del cloud computing:

- **Self-service on demand:** gli utenti possono autonomamente richiedere e ottenere risorse informatiche, come tempo del server e storage di rete, in base alle proprie esigenze, in modo automatico e senza la necessità di interagire con il fornitore di servizi.
- **Ampio accesso alla rete:** le funzionalità del cloud sono disponibili attraverso la rete e accessibili tramite meccanismi standard che ne promuovono l'utilizzo da parte di piattaforme client eterogenee, come telefoni cellulari, tablet, laptop e workstation.
- **Resource pooling:** le risorse informatiche del fornitore sono condivise tra più utenti, con diverse risorse fisiche e virtuali assegnate dinamicamente in base alla domanda. Il cliente non ha controllo sulla posizione esatta delle risorse fornite, ma può essere in grado di specificare la posizione a un livello di astrazione più elevato (ad esempio, paese, stato o data center).
- **Rapid Elasticity:** le funzionalità possono essere fornite e rilasciate in modo elastico, in alcuni casi automaticamente, per adattarsi rapidamente ai cambiamenti nella domanda, questo fa sì che il cliente abbia l'impressione che i servizi disponibili e le risorse siano illimitate.
- **Measured e Reporting Service:** i sistemi cloud controllano e ottimizzano automaticamente l'utilizzo delle risorse, L'utilizzo delle risorse può essere monitorato, controllato e segnalato dal fornitore, ma anche dal cliente stesso, poiché l'unità di misura adottata per controllare il consumo delle risorse è trasparente ed accessibile anche all'utente del servizio utilizzato.

- **Facilità di aggiornamento:** le risorse basate sul Cloud Computing sono soggette ad aggiornamenti frequenti, tali aggiornamenti vengono effettuati dai Cloud provider, in questo modo viene ottimizzata la capacità e il potenziale del servizio.
- **Multi-Tenancy**: è un'architettura software che consente ad una singola istanza di programma di servire diversi gruppi di utenti. Anche se più clienti di un CSP condividono le stesse risorse, i dati di ciascun cliente sono tenuti completamente separati.

Queste sono le caratteristiche che hanno permesso una rapida diffusione del cloud computing nel mondo aziendale, prima fra tutte la possibilità di scalare velocemente, l'abbattimento dei costi iniziali e la trasformazione dei costi fissi "Cap-ex" in "Op-ex", ciò permette alle aziende di avere rapido accesso alle tecnologie di cui necessitano portando ad una riduzione del time to market. L'innovazione continua garantita e gestita direttamente dai provider e la possibilità di concentrarsi sul core business. Contestualmente la scelta di affidarsi ad un provider cloud, dall'altro lato, comporta alcune sfide da affrontare come la dipendenza dal provider per i livelli di affidabilità, di sicurezza e la conformità normativa. Ad oggi le applicazioni aziendali sono un elemento fondamentale per un'organizzazione pertanto è necessario che siano affidabili e sempre disponibili. Per quanto riguarda la normativa vigente, si fa riferimento a quella del paese di ubicazione dei data center, la complessità sui temi normativi è data dal fatto che nel mondo del cloud l'infrastruttura è distribuita su diverse regioni geografiche pertanto a causa di questa variabilità, possono applicarsi diversi regolamenti sulla privacy. Ovviamente tutto ciò assume un peso sempre più preponderante quando si parla di settori con stringenti normative sulla protezione dei dati (come per esempio il settore sanitario o quello finanziario). Un altro fattore estremamente rilevante da valutare sono gli effetti di Lock-in, a causa dei quali il passaggio ad un altro provider o il ritorno ad un'infrastruttura on-premis diventa molto costoso.

TREND DI CRESCITA NEL MERCATO DEL CLOUD COMPUTING

Il mercato del cloud computing è uno dei mercati in più rapida crescita al mondo oggi. Si prevede che il mercato globale del cloud computing, che nel 2022 era di 446,51 miliardi di dollari, raggiungerà i 1.614,10 miliardi di dollari entro il 2030. Inoltre la quantità totale di dati archiviati nel cloud, che include i cloud pubblici gestiti da fornitori e aziende di social media (ad esempio Apple, Facebook,

Google, Microsoft, Twitter, ecc.), i cloud di proprietà governativa accessibili a cittadini e aziende, i cloud privati di proprietà di aziende di medie e grandi dimensioni e i provider di storage cloud, raggiungerà i 100 zettabyte entro il 2025, ovvero il 50 percento dei dati mondiali di quel momento, rispetto al 25 percento circa archiviato nel cloud nel 2015.

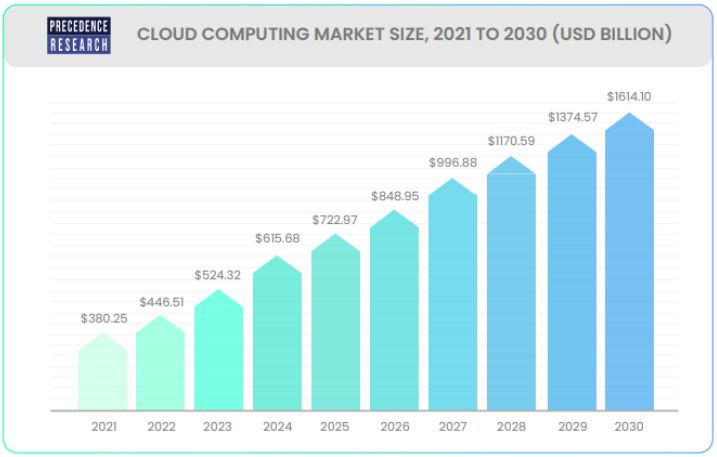

Figura 3: Trend di crescita del cloud computing

Con questa crescita esponenziale dei dati, le opportunità (per l'innovazione e per la criminalità informatica) sono incalcolabili.

1.4 I MODELLI DI SERVIZIO DI CLOUD COMPUTING

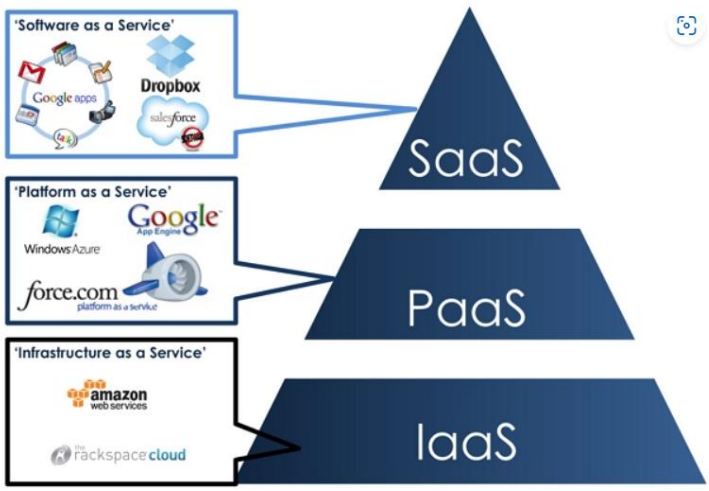

Figura 4: Modelli di Servizio

SOFTWARE AS A SERVICE (SAAS)

In questo modello, il fornitore offre all'utente un'applicazione software eseguita su un'infrastruttura cloud, è la tipologia di servizio più completa in quanto l'utente finale non deve sviluppare da sé l'applicazione, non deve gestire né controllare il sistema operativo e l'infrastruttura hardware sottostante pertanto non sono necessarie delle competenze informatiche. Può accedere ed utilizzare l'applicazione da vari dispositivi tramite un'interfaccia thin, come un browser web (ad esempio, la posta elettronica basata sul web).

- Il principale vantaggio è la possibilità di usare i servizi su qualsiasi dispositivo e in qualsiasi luogo.
- Al tempo stesso l'utente ha un controllo limitato sull'applicazione, sulla configurazione e la personalizzazione delle applicazioni.

Questa tipologia di servizi viene spesso erogata con strategie freemium oppure può richiedere una sottoscrizione basata sul tempo di utilizzo. Esempi di SaaS sono: Google G Suite (Gmail, Google Drive, Google Planner), Microsoft Office 365, Salesforce: il CRM5 è l'applicazione più utulizzata sul mercato, utilizzata dagli imprenditori per tenere traccia delle vendite, dei rapporti commerciali con clienti e fornitori, ed in generale delle attività pertinenti al business, accessibile da ogni dispositivo.

Il modello Software-as-a-Service (SaaS), conosciuto anche come servizi applicativi Cloud, è la forma più completa di servizi di Cloud Computing in quanto fornisce un'applicazione interamente gestita e ospitata dal provider, accessibile direttamente tramite un browser web.

PLATFORM AS A SERVICE (PAAS)

Può essere visto come una piattaforma intermedia tra il modello (SaaS) e quello (IaaS). In questo caso, l'utente ha la possibilità di sviluppare e configurare l'applicazione secondo le sue necessità ma senza doversi preoccupare dell'hardware sottostante (rete, server, sistemi operativi o storage). Questa tipologia di cloud è più adatta per gli sviluppatori, sono necessarie quindi delle competenze informatiche per lo sviluppo in quanto sono richiesti specifici linguaggi di programmazione per implementare l'app, ma questo d'altro canto permette all'utente di avere pieno controllo sull'applicazione e al tempo stesso sfruttare gli aggiornamenti e la scalabilità del cloud computing.

- Il principale vantaggio quindi è la *scalabilità e l'affidabilità* garantita dai provider Paas che gestiscono l'infrastruttura, la possibilità di concentrarsi sulla creazione e implementazione delle applicazioni senza doversi preoccupare dell'infrastruttura sottostante.
- Lo svantaggio principale è rappresentato dalla limitazione delle risorse che viene imposta dai provider e questo può influire sulle prestazioni delle applicazioni in caso di carichi di lavoro elevati. Come anche la minore flessibilità, infatti i provider offrono un insieme limitato di strumenti e tecnologie per cui gli sviluppatori devono adeguarsi all'offerta.

Esempi di provider PaaS includono Google App Engine (GAE) e AWS Elastic Beanstalk.

INFRASTRUCTURE AS A SERVICE (IAAS)

In questo modello, il fornitore offre all'utente risorse informatiche di base come elaborazione, storage e reti, consentendogli di creare il proprio datacenter virtuale /vDC), in questo il cliente ha a disposizione tutta la flessibilità che potrebbe ottenere da un'infrastruttura fisica proprietaria. Ha infatti, il controllo sui sistemi operativi e sull'intero sviluppo dell'applicazione, senza l'onere della gestione e della manutenzione dell'harware. L'utente può quindi implementare ed eseguire *qualsiasi software* desideri su queste risorse, inclusi sistemi operativi e applicazioni, mantenendo il pieno controllo sui sistemi operativi, sullo storage e sulle applicazioni implementate.

- I vantaggi più importanti sono legati sicuramente alla flessibilità e al controllo, infatti Iaas offre il massimo livello di *flessibilità e controllo* sull'infrastruttura IT. Gli utenti possono scegliere e configurare i sistemi operativi, le applicazioni e le risorse di rete in base alle proprie esigenze specifiche, inoltre le risorse IaaS possono essere adeguate in base alle esigenze (scalabilità on-demand) consentendo alle aziende di adattarsi alle variazioni del carico di lavoro e di pagare solo per le risorse effettivamente utilizzate.
- Il principale svantaggio è la maggiore complessità di gestione, pertanto sono necessarie le competenze tecniche di alto livello. Infatti, gli utenti IaaS sono responsabili della gestione e del mantenimento dei sistemi operativi, delle applicazioni e della sicurezza.

Esempi di provider IaaS includono Amazon Web Services (AWS), Google Cloud Platform (GCP) e Microsoft Azure.

IaaS Versus PaaS Versus SaaS			
	IaaS	**PaaS**	**SaaS**
Application	User managed	User managed	Provider managed
Data	User managed	User managed	Provider managed
Runtime and middleware	User managed	Provider managed	Provider managed
Operating system	User managed	Provider managed	Provider managed
Server virtualization	Provider managed	Provider managed	Provider managed
Hardware	Provider managed	Provider managed	Provider managed

Figura 5: Le responsabilità del provider e degli utenti nei tre modelli di servizio

Questa immagine fornisce una rappresentazione chiara e concisa di come siano suddivisi i ruoli e quindi le responsabilità nei diversi modelli di servizio. Possiamo vedere subito come nel caso dell'Iaas soltanto le funzioni più di basso livello, in termini informatici, siano gestite dal provider. Invece man mano che ci spostiamo verso il Saas tutte le funzionalità vengono gestite dal provider. La scelta di quale servizio utilizzare e se adottarne diversi contemporaneamente dipende dalle esigenze e dalla tipologia di azienda in questione.

1.5 MODELLI DI DEPLOYMENT

Oltre ai modelli di servizio, esistono anche diversi modelli di deployment per il cloud computing:

- **Cloud pubblico**: I cloud pubblici sono ambienti cloud basati su un'infrastruttura IT che solitamente non appartiene all'utente finale e che viene aperta al pubblico in generale. L'infrastruttura può essere gestita o operata da un'organizzazione aziendale, accademica o governativa, o da una combinazione di esse.

I provider di cloud pubblico più rilevanti sono: Amazon Web Services (AWS), Google Cloud, Microsoft Azure, Alibaba Cloud e IBM Cloud.

- **Cloud privato**: l'infrastruttura cloud viene utilizzata da una singola organizzazione che comprende più fruitori (ad esempio, unità aziendali). Può essere di proprietà, gestita e sviluppata dall'organizzazione, da terzi o da una combinazione di esse e può esistere on premise o off premise, infatti non è più necessario che i cloud privati vengano implementati

in un'infrastruttura IT on premise. Le organizzazioni possono realizzare i propri cloud privati su datacenter in affitto, ovvero di proprietà del fornitore e ubicati off premise. In questo senso, la distinzione in base a ubicazione e titolarità diventa obsoleta. Questa strutturazione genera diversi sottotipi di cloud privato, tra cui:

  - **Cloud privato gestito**: Permettono di creare e usare un cloud privato che viene implementato, configurato e gestito da un fornitore terzo. I cloud privati gestiti sono un'alternativa adatta alle aziende che non hanno personale IT specializzato poiché consentono loro di offrire servizi di cloud privato e infrastrutture migliori ai clienti.
  - **Cloud dedicato**: Un cloud contenuto in un altro cloud. Può esistere all'interno di un cloud pubblico o di un cloud privato. Ad esempio, il reparto contabilità di un'azienda può utilizzare il proprio cloud dedicato, ubicato all'interno del cloud privato aziendale.

- **Cloud ibrido**: l'infrastruttura cloud è data dall'insieme di due o più infrastrutture cloud distinte (private, community o pubbliche) che rimangono entità uniche, connesse tramite reti LAN (Local Area Network), WAN (Wide Area Network) o VPN (Virtual Private Network). Quindi un cloud ibrido combina elementi di cloud pubblico e privato. Questa soluzione è molto popolare tra le aziende, poiché in questo modo possono utilizzare un cloud privato per le operazioni critiche e un cloud pubblico per le attività meno sensibili.
- **Ambiente multicloud**: è costituito da più di un servizio cloud e da più di un operatore di servizi cloud, pubblici o privati ciò non implica che i dati debbano essere necessariamente condivisi tra di esse, questa è la differenza fondamentale tra un cloud ibrido e un ambiente multicloud. Infatti, il cloud ibrido presuppone l'ambiente multicloud ma non è necessariamente vero il contrario questo perché una configurazione multicloud può essere resa ibrida, ma può esistere anche se i singoli ambienti cloud non comunicano tra loro. L'ambiente multicloud ha un livello di affidabilità maggiore rispetto ad un ambiente singolo poiché contiene informazioni ridondanti, ciò consente di migliorare il ripristino di emergenza e controllare più efficacemente i dati sensibili, ma può formarsi anche accidentalmente, in seguito all'utilizzo dello shadow IT. Pertanto la scelta di utilizzare un ambiente multicloud dipende dal tipo di informazioni trattate e il livello di sicurezza che si vuole ottenere.

- **Cloud community**: l'infrastruttura cloud è fornita per l'uso esclusivo da parte di una specifica community di utenti, di organizzazioni che condividono preoccupazioni comuni (ad esempio, mission, requisiti di sicurezza, policy e considerazioni sulla conformità). Può essere di proprietà, gestita da una o più organizzazioni della community, da terzi o da una combinazione di esse e può esistere in loco o fuori sede

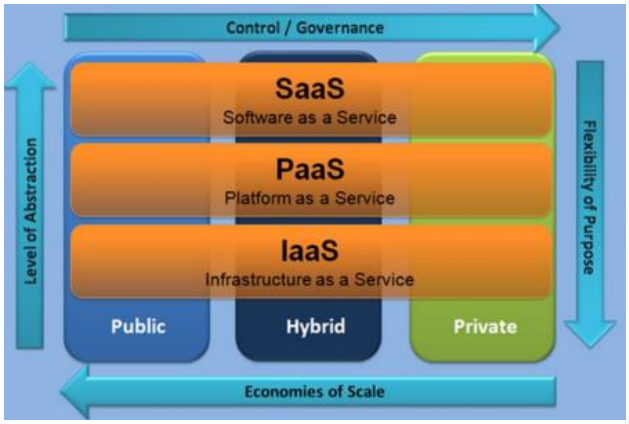

Figure 6: Interazione tra modelli di servizio e di deployment

Dall'interazione tra i diversi modelli di servizio e di deployment le aziende ottengono diversi livelli di controllo, flessibilità ed economie di scala. Di contro i provider devono gestire diversi livelli di astrazione. Infatti il con il cloud pubblico si raggiungono le maggiori economie di scala poiché la stessa (grande) infrastruttura viene condivisa da moltissime organizzazioni pertanto si raggiunge la massima efficienza operativa, che invece si riduce man mano che ci spostiamo verso il cloud privato che molto spesso deve essere sovradimensionato ed è utilizzato da una sola organizzazione (anche se con più unità aziendali, l'efficienza raggiunta non è paragonabile a quella di un cloud pubblico). Invece, il controllo e la governance si muovono in verso totalmente opposto, come abbiamo già visto quando abbiamo parlato di cloud privato, sia nel caso on premis che off premis, l'organizzazione ha il pieno controllo sulla localizzazione dei dati, sul disaster recovery e così via.

1.6 EDGE COMPUTING

L'edge computing è un nuovo modello di servizio in risposta all'evoluzione delle esigenze dei clienti. Con l'aumento dell'**Internet of Things (IoT)**, sempre più dispositivi generano enormi quantità di dati in tempo reale, che devono essere elaborati in modo rapido. I servizi cloud rispondono a questa

esigenza “avvicinandosi” al luogo in cui i dati vengono generati o raccolti, l’edge computing infatti, è un’architettura distribuita in cui l’elaborazione delle informazioni avviene nei pressi della loro sorgente, anziché in un cloud centralizzato. Grazie all’elaborazione locale, il dispositivo può prendere decisioni in tempo reale. Analogamente al cloud ibrido, che permette alle organizzazioni di eseguire i carichi di lavoro sia in propri data center ma anche sulle infrastrutture di cloud pubblico, allo stesso modo l’edge computing permette di distribuire un ambiente cloud dal datacenter centrale a posizioni fisiche vicino agli utenti e ai dati. L’edge computing è utilizzato in diversi settori, per esempio nelle telecomunicazioni, trasporti, servizi pubblici. Inoltre il report “the economic potential of far edge computing in the future smart Internet of Things” mette in evidenza come l’Unione Europea, sfruttando la sua forza nell’IoT professionale in settori come l’automotive, sicurezza e sanità, potrebbe sviluppare una posizione di leadership nelle piattaforme dell’Edge computing. Pertanto l’Edge computing rappresenta un’opportunità strategia per l’UE per promuovere la crescita economica, la sostenibilità ambientale e raggiungere la sovranità digitale. Per raggiungere questo obiettivo sono necessarie la collaborazione tra i diversi attori europei, la standardizzazione, e l’innovazione.

Inoltre secondo quanto previsto nel programma “DECISION (EU) 2022/2481 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of December 14, 2022, establishing the strategic programme for the digital decade 2030” vediamo come la sostenibilità ambientale sia un tema centrale per l’UE nell’ambito della trasformazione digitale ed in particolare dell’Edge computing, infatti tra gli obiettivi principali troviamo l’installazione di 10.000 nodi periferici ad impatto climatico nullo, garantendo l’accesso a servizi di dati a bassa latenza in modo sostenibile. Inoltre promuove la produzione di semiconduttori a bassa latenza ed impronta energetica così da rafforzare contemporaneamente la posizione di leadership dell’UE nelle tecnologie digitali sostenibili e al tempo stesso ridurre la dipendenza da fornitori extra-UE.

Esempi di Applicazioni dell'Edge Computing

- **Auto a Guida Autonoma**: I sensori e le telecamere delle auto generano dati che devono essere processati istantaneamente in modo tale da prendere decisioni in tempo reale che garantiscano la sicurezza del sistema.

- **Smart Cities**: Nelle città intelligenti, i sensori per la gestione del traffico, dell'illuminazione pubblica o dei parcheggi usano l'edge computing per gestire i dati e processarli in tempo reale.
- **Industria 4.0**: Nei contesti di produzione industriale, i macchinari connessi possono rilevare difetti di funzionamento e attivare interventi di manutenzione predittiva, riducendo il rischio di guasti e migliorando il tasso di affidabilità del sistema.
- **Healthcare**: Dispositivi medici intelligenti, come i monitor cardiaci, usano l'edge computing per monitorare i segni vitali e avvisare in caso di anomalie.

1.7 PROVIDER CLOUD

I principali fornitori di servizi di cloud computing al mondo sono: *Amazon, Microsoft e Google* che attualmente controllano il 66% del mercato globale. I tre big player generano miliardi di fatturato tramite la loro infrastruttura cloud che fornisce la potenza di calcolo di cui le aziende hanno bisogno per archiviare i dati e non solo. Inoltre, adesso la maggior parte dei modelli di intelligenza artificiale viene eseguita sul cloud, creando un'impennata nella domanda di elaborazione per i provider cloud.

Figura 7: Magic Quadrant for Strategic Cloud Platform services

AMAZON WEB SERVICES

Amazon Web Services (AWS) è una piattaforma cloud che offre diversi servizi full-feature, attualmente più di 200, si passa dallo storage all'elaborazione dei dati, quindi strumenti di analisi, strumenti per sviluppatori, la sicurezza e i servizi dedicati ai dispositivi ioT. Sono infatti pensati per realizzare qualsiasi progetto IT in cloud per aziende di tutte le dimensioni. AWS presenta regioni distribuite in tutto il mondo, una grande elasticità e affidabilità che di fatto lo rendono l'ecosistema cloud più completo e utilizzato. Ha esperienza e competenza senza pari nel panorama del cloud e milioni di clienti attivi a livello globale, passiamo infatti da startup a grandi imprese fino ad agenzie governative che reputano AWS il provider ottimale per diminuire i costi, operare in modo più agile e accelerare la propria innovazione.

Vantaggi:

- **Servizi**: AWS offre un numero elevato di servizi e funzionalità che spaziano dalle tecnologie infrastrutturali (come elaborazione, storage e database) alle tecnologie emergenti (come apprendimento automatico e intelligenza artificiale)
- **Comunità di clienti e partner**: AWS ha una delle community più grandi, con milioni di clienti attivi e decine di migliaia di partner in tutto il mondo. Clienti di praticamente ogni settore e di ogni dimensione eseguono qualsiasi caso d'uso immaginabile su AWS.
- **Sicurezza**: L'infrastruttura è costruita per soddisfare i requisiti di sicurezza per l'esercito, le banche e altre organizzazioni ad alta sensibilità. Questo grazie ad un profondo set di strumenti di sicurezza cloud, conformità agli standard di sicurezza, certificazioni e meccanismi di crittografia.
- **Comprovata esperienza operativa**: AWS ha un'esperienza ineguagliabile. Infatti, da oltre 10 anni AWS fornisce servizi cloud a milioni di clienti in tutto il mondo che lo utilizzano per svolgere diversi casi d'uso.

Svantaggi:

- AWS non ha una politica di prezzi molto conveniente, infatti nonostante faccia frequenti proclami su **riduzioni di prezzo**, queste poi non si realizzano. Ad esempio, l'archiviazione predefinita e più frequentemente fornita per il servizio di elaborazione di AWS non ha subito una riduzione di prezzo dal 2014, nonostante la diminuzione dei prezzi sul mercato per i componenti grezzi.
- AWS privilegia la **velocità di commercializzazione** rispetto all'offerta di nuovi servizi e funzionalità. Di conseguenza, è disposta a lanciare servizi con funzionalità non ottimali o servizi senza una profonda integrazione multipiattaforma. Ciò si traduce in servizi che richiedono anni di sostanziali aggiornamenti ingegneristici.

MICROSOFT AZURE

Microsoft Azure è la piattaforma di cloud computing pubblica di Microsoft, è un insieme in continua espansione di servizi, che aiutano le organizzazioni a fronteggiare le sfide aziendali. Microsoft Azure si è affermata come piattaforma leader per sviluppatori, offre loro la libertà di creare, gestire e distribuire applicazioni su una rete globale vasta, utilizzando un'ampia gamma di strumenti e framework. Beneficia dell'eccellente integrazione con i prodotti e strumenti per sviluppatori Microsoft ed offre soluzioni cloud ibride che soddisfano le esigenze delle aziende che insieme alle robuste funzionalità di sicurezza lo hanno reso uno dei leader del mercato. Azure offre una vasta gamma di servizi, tra cui:

- Calcolo: Azure offre una varietà di servizi di elaborazione, tra cui macchine virtuali
- Archiviazione: Azure offre una varietà di servizi di archiviazione
- Database: Azure offre una varietà di servizi di database, tra cui database SQL, database NoSQL e cache.
- Analisi: Azure offre una varietà di servizi di analisi, tra cui analisi in tempo reale e apprendimento automatico

Questi servizi possono essere utilizzati per creare e implementare un'ampia gamma di applicazioni, da semplici app Web a sistemi aziendali complessi. I suoi punti di forza sono:

- **Portata globale**: Con data center in più regioni (58) rispetto a qualsiasi altro provider di cloud, Azure offre una presenza locale di cui molte aziende e organizzazioni hanno bisogno. Ciò consente loro di ridurre i costi, i tempi e la complessità della gestione di un'infrastruttura globale, soddisfacendo al contempo le esigenze locali di residenza dei dati.
- **Focus sul cloud Ibrido**: Azure si distingue per la sua attenzione al cloud ibrido, che molto spesso risulta la soluzione più adatta per risolvere i problemi di privacy da un lato e scalabilità e flessibilità dall'altro. In questo modo Azure aiuta le aziende a colmare a colmare questo divario, grazie al suo ambiente ricco di funzionalità e rapidamente scalabile e alla suite di strumenti e servizi progettati per il cloud ibrido consente una perfetta integrazione.
- **Sicuro**: Azure propone un approccio proattivo alla sicurezza, alla conformità e alla privacy. Microsoft dimostra il suo impegno incessante nello stabilire e soddisfare costantemente chiari requisiti di sicurezza e privacy con innumerevoli certificazioni di conformità e privacy, i controlli di sicurezza integrati e l'esclusiva Threat Intelligence. In questo modo Azure offre tutto ciò che serve per identificare e proteggersi dalle minacce in rapida evoluzione e ciò lo rende leader del settore.
- **Flessibilità dello sviluppo**: Azure abbraccia l'apertura, supportando strumenti e framework open source, vari linguaggi di programmazione e framework, offrendo agli sviluppatori la flessibilità di creare secondo le proprie preferenze e condizioni.

Punti deboli di Microsoft Azure

- **Affidabilità**: I problemi di affidabilità di Microsoft Azure continuano a rappresentare una sfida per i clienti, in gran parte a causa dei problemi di crescita di Azure. Da settembre 2018, Azure ha avuto diversi incidenti che hanno avuto un impatto sul servizio. La natura di molte di queste interruzioni è tale che i clienti non avevano il controllo per mitigare i tempi di inattività.

- **Supporto**: Le aziende spesso non sono soddisfatte della qualità del supporto tecnico offerto da Microsoft (che risulta sempre più costoso) e delle soluzioni sul campo. Ciò ha un impatto negativo sulla reputazione di Microsoft e rallenta l'adozione di Azure e la spesa dei clienti.

GOOGLE CLOUD PLATFORM

Il terzo grande player del cloud è Google Cloud Platform (GCP). Mentre AWS si concentra principalmente sul cloud pubblico e Azure eccelle nel cloud ibrido, GCP è noto per la sua competenza tecnica, in particolare nei settori del deep learning, dell'intelligenza artificiale, dell'apprendimento automatico e dell'analisi dei dati. GCP eccelle anche in offerte di calcolo elevate come big data, analisi e machine learning, oltre a fornire scalabilità e bilanciamento del carico significativi. GCP offre una vasta gamma di servizi, tra cui hosting e elaborazione, archiviazione cloud, archiviazione dati, API di traduzione e API di previsione. Con 19 categorie separate di software cloud, GCP offre probabilmente il miglior portafoglio dei tre principali fornitori di cloud. GPC è ospitato sulla stessa infrastruttura utilizzata da Google per prodotti come Google Search e YouTube.

Punti di forza

- GCP offre prezzi competitivi, infatti è considerato più competitivo rispetto ad AWS ed Azure inoltre introduce innovazioni come la fatturazione al minuto e l'utilizzo continuativo.
- Ha una forte attenzione alla sicurezza: GCP è protetto da oltre 700 esperti di sicurezza informatica, delle applicazioni e della rete.
- GCP è in continua evoluzione, con nuove funzionalità e servizi aggiunti regolarmente.
- Sostenibilità ambientale: GCP ha il punteggio di sostenibilità più alto tra i provider nel Magic Quadrant. Ciò diventa estremamente rilevante per i clienti che utilizzano il cloud per attività altamente energivore come l’allenamento di modelli AI che richiedono grandi quantitativi di immagini e iterazioni conitinue

GCP presenta anche alcune **debolezze**

- Carenze nei contratti aziendali: GCP è stato criticato per la sua immaturità nelle aree della negoziazione dei contratti, degli sconti, delle licenze dei fornitori di software indipendenti, dell'integrazione con i sistemi aziendali e del supporto. Questo perché GCP nasce e si sviluppa indirizzandosi allo sviluppatore che “da solo” crea la sua idea di successo. Questo ha portato GCP a concentrarsi in ritardo sul mercato aziendale. Infatti, la copertura aziendale complessiva di Google dal punto di vista delle vendite sul campo e delle soluzioni è inferiore a quella dei suoi concorrenti, il che rende più difficile per le aziende adottare e utilizzare GCP.
- Ecosistema di partner limitato: GCP ha un pool di partner di servizi professionali incentrati su MSP e infrastrutture molto più piccolo rispetto ad altri fornitori. Pertanto i clienti potrebbero avere maggiori difficoltà nel trovare consulenti o partner esperti che li aiutino a configurare e gestire GPC
- Google mantiene un programma di migrazione dei clienti (RaMP) completo e in espansione, con oltre 70 partner di migrazione certificati. Tuttavia il progetto di migrazione di Google Cloud per alcuni clienti è stato ostacolato dalla **mancanza di disponibilità** del team degli account Google o dalla **mancanza di esperienza** approfondita dei partner con GCP.
- Integrazione minima tra Google Cloud e altri prodotti Alphabet: GCP non è strettamente integrato con le altre proprietà basate sul cloud di Google, in particolare Workspace, né con gli altri prodotti della sua società madre Alphabet. I clienti che sperano di utilizzare GCP come base per comporre soluzioni digitali nel portafoglio Google troveranno attualmente poco supporto immediato e potrebbero dover negoziare termini commerciali con più unità aziendali di Google.

Nonostante queste sfide, GCP è una piattaforma cloud potente e ricca di funzionalità che offre una vasta gamma di vantaggi alle aziende di tutte le dimensioni.

1.8 NICHE PLAYERS

ALIBABA CLOUD

Alibaba Cloud nasce e si sviluppa, in Cina e in Asia, in cui era ed è il principale mercato online. Nel 2009 l'infrastruttura venne aperta al pubblico sotto il nome di Aliyun. Successivamente, nel 2015, decisero di espandersi al di fuori della Cina, pertanto potenziarono l'infrastruttura e crearono quello che oggi conosciamo come Alibaba Cloud. Alibaba Cloud offre tutti i servizi alle aziende cinesi per "diventare globali" utilizzando la sua infrastruttura cloud internazionale. Tuttavia, non tutti questi servizi sono disponibili a livello internazionale.

Punti di forza

- Leadership di mercato in Cina: Alibaba Cloud è leader di mercato nel cloud in Cina, e questo ha una ricaduta sulla sua influenza internazionale, infatti l'ecosistema di partner di Alibaba Cloud e la sua leadership nella comunità open source in Cina gli conferiscono un maggior peso nei mercati circostanti, come il Sud-Est asiatico.
- Infrastruttura ibrida e capacità ingegneristica: il talento ingegneristico di Alibaba Cloud è evidente nell'ampiezza e nella profondità delle funzionalità delle sue soluzioni cloud private.
- L'attenzione verso la sostenibilità: i progetti di sostenibilità di Alibaba Cloud hanno anche migliorato la valutazione dell'efficacia dell'utilizzo di energia (Power Usage Effectiveness) dei suoi data center.
- Abilitazione dell'ecosistema digitale: Alibaba Cloud sfrutta l'influenza della sua casa madre, Alibaba Group, per offrire opzioni di business digitale che i suoi concorrenti non possono eguagliare. Tra queste rientrano l'accesso alla rete commerciale di Alibaba e ai servizi Internet più popolari, come DingTalk e Alipay. Queste capacità vengono sfruttate soprattutto dalle aziende cinesi che si espandono nei mercati internazionali.

Punti di debolezza

- Incertezza strategica: a maggio 2023, Alibaba Cloud ha avviato licenziamenti limitati. A settembre, il CEO Daniel Zhang si è dimesso inaspettatamente dopo pochi mesi di ruolo. Questa

mancanza di stabilità, unita alla mancanza di un piano di finanziamento pubblico o privato confermato, trasmette incertezza ai clienti e agli investitori.

- Offerte di servizi e supporto globali limitati a livello internazionale: molti servizi cloud disponibili da Alibaba Cloud in Cina non sono disponibili o lo sono solo in parte nelle regioni internazionali. Al di fuori della Cina, il supporto e la presenza dei partner di Alibaba Cloud sono limitati. Inoltre anche le prestazioni risultano inferiori nel mercato internazionale. Ciò è dovuto alle restrizioni commerciali occidentali contro la Cina su tecnologie chiave come le GPU NVIDIA. Pertanto questa potrebbe essere una delle cause per cui Alibaba non riesce a competere a pieno al di fuori del territorio cinese.

IBM

Tra i Niche Player del Magic Quadrant di Gartner troviamo anche IBM. Le operazioni di IBM Cloud sono diversificate geograficamente e focalizzate su servizi IaaS, e relativi ai dati. Si basano su tecnologie open source come Red Hat OpenShift che dal 2019, anno dell'acquisizione. Rispetto ad altri fornitori ha un approccio diverso al go-to-market, offre infatti la possibilità ai suoi clienti di ottenere soluzioni complete e personalizzate tramite un impegno di servizio con IBM Consulting o un partner locale, inoltre include tutte le tecnologie di ultima generazione che gli permettono di accelerare il processo di modernizzazione e supportare al meglio le aziende e le loro esigenze. IBM cloud in generale si concentra principalmente sul cloud ibrido e sui settori regolamentati e i clienti di IBM tendono a essere grandi e medie imprese con investimenti esistenti in altre tecnologie IBM.

Punti di forza

- IBM ha opzioni personalizzate per soddisfare i requisiti di settori altamente regolamentati come i servizi finanziari. Ad esempio, IBM Cloud for Financial Services include set di controllo pre-configurati per supportare la conformità automatizzata e la sicurezza per i carichi di lavoro più sensibili.
- Gestione dei container multi-cloud: IBM basa la sua offerta su Red Hat OpenShift, consentendo ai clienti di implementare la loro strategia di container su una piattaforma popolare che abbraccia sedi ibride e multicloud. OpenShift è fondamentale per la strategia

cloud di IBM e funge da base per la distribuzione del software IBM su provider come AWS e Microsoft Azure tramite le loro offerte con marchio congiunto.

Punti di debolezza

- Affidabilità: dal 2021 al 2023, IBM ha profuso notevoli sforzi per migliorare l'affidabilità, con conseguente notevole riduzione degli incidenti dirompenti. Tuttavia, anche con tali miglioramenti, l'architettura di resilienza di IBM Cloud non è all'altezza di altri leader nel mercato dei servizi di piattaforma cloud strategica (SCPS).
- Mancanza di un'architettura cloud unificata: nonostante abbia lanciato la sua infrastruttura Gen2 IBM Cloud VPC nel 2019, IBM continua a vendere, supportare e migliorare il suo ambiente Gen1 (IBM Cloud Classic). Inoltre, i principali strumenti di gestione cloud acquisiti da IBM per l'uso in IBM Cloud VPC, come Instana e Turbonomic, non sono completamente integrati in IBM Cloud Management Console e devono essere acquistati e distribuiti separatamente.
- Supporto limitato da parte degli MSP: i principali provider di servizi gestiti dal cloud offrono solo un supporto limitato per IBM Cloud. I clienti che cercano una trasformazione e operazioni gestite su IBM Cloud devono affidarsi a partner locali o sviluppare tali competenze internamente.

I FORNITORI CLOUD

Guardando al mercato del cloud in generale e alle loro quote di mercato, possiamo notare come questo sia un mercato altamente concentrato: si passa da AWS che domina il mercato con una quota pari al 32% ad Alibaba Cloud in quarta posizione con soltanto il 4%.

Azienda	Sede centrale	Quota di mercato	Ricavo annuo
Servizi Web Amazon (AWS)	Washington, Stati Uniti	32%	≈$80 miliardi di euro
Microsoft Azure	Redmond, Stati Uniti	22%	≈$34 miliardi di euro
Piattaforma cloud di Google (GCP)	California, Stati Uniti	11%	≈$7,4 miliardi di euro
Oracle Cloud	Texas, Stati Uniti	2%	≈$5,8 miliardi di euro
IBM Cloud	New York, Stati Uniti	3%	≈$22 miliardi di euro
Alibaba Cloud	Distretto di Yu Hang, Cina	4%	≈$12 miliardi di euro
Salesforce Cloud	California, Stati Uniti	3%	≈$33,07 miliardi di euro
Rackspace	Texas, Stati Uniti	0.96%	≈$3,1 miliardi di euro
Digital Ocean	New York, Stati Uniti	1.55%	≈$650 milioni di euro
OVHCloud	Roubaix, Francia	<1%	≈$220 milioni di euro

Figure 8: Confronto tra i CSP

1.9 CONCENTRAZIONE DEL MERCATO

Avere una quota di mercato elevata non implica necessariamente distorcere il mercato, escludere i nuovi entranti o mantenere il potere monopolistico. Tuttavia, nel caso del mercato del cloud si osserva che le aziende leader dominano il mercato, lasciando poco spazio ai competitors con ovvi effetti negativi sulla competizione. L'indice di Herfindahl-Hirschman (HHI), calcolato sommando i quadrati delle quote di mercato di tutte le aziende del settore, testimonia questo alto livello di concentrazione con un valore pari a 3.457.

$$H = \sum_{i=1}^{N} S_i^2$$

Questo fenomeno può verificarsi per vari motivi secondo il Digital Market Act (Considerando 2)

"In questi sistemi di piattaforme digitali (CPS), le grandi *economie di scala*, gli *effetti di rete diretti* e indiretti e i *vantaggi derivanti dall'uso dei dati* possono influire negativamente sull'equità nelle

relazioni commerciali tra le imprese che forniscono tali servizi e i loro utenti commerciali e finali, nonché sulla contestabilità e sulle dinamiche di concorrenza, causando effetti di lock-in e mancanza di multihoming, sia a livello delle piattaforme (a monte) sia nel mercato degli utenti commerciali. Questo fenomeno si verifica soprattutto quando i fornitori di piattaforme digitali sono integrati verticalmente (o orizzontalmente)".

Infatti, quando una grande azienda domina il mercato, essa possiede spesso un forte posizionamento di mercato e un vantaggio competitivo. Di conseguenza, i piccoli operatori del cloud potrebbero trovare difficile entrare nel mercato, stabilire competitività e aumentare la propria quota di mercato. Un tale scenario può ostacolare la crescita di nuovi entranti e di imprese su piccola scala. Inoltre, il dominio di mercato da parte di pochi attori può comportare barriere all'entrata più elevate. Le grandi aziende hanno vantaggi in termini di capitale e quindi economie di scala, tecnologia e valore del marchio, rendendo difficile per le imprese più piccole superare queste barriere all'entrata. Di conseguenza, le opportunità per vari partecipanti al mercato del cloud di competere e innovare potrebbero diventare limitate. Inoltre il mercato del cloud computing è caratterizzato dall'assenza di interoperabilità tra i diversi provider, il che insieme ad altri fattori provoca il lock-in degli utenti, portando ad una riduzione della pressione competitiva e alla concentrazione del mercato.

Per esempio nel caso di Google, la sua posizione dominante nel mercato del cloud deriva da vari fattori chiave che includono:

- Economie di scala: Google possiede una vasta infrastruttura tecnologica, con enormi capacità di archiviazione e calcolo grazie ai suoi data center distribuiti a livello globale. Questo gli consente di offrire servizi cloud su una scala che i concorrenti più piccoli non possono raggiungere facilmente, riducendo così i costi e aumentandone l'efficienza.
- Accesso ai dati su larga scala: Uno dei principali punti di forza di Google è l'accesso ai dati degli utenti. Ogni giorno, milioni di persone usano servizi come Google Search, Gmail, Google Maps e YouTube, fornendo a Google una quantità immensa di informazioni. Questo flusso continuo di dati alimenta i suoi algoritmi di intelligenza artificiale e migliora la qualità e l'efficienza dei servizi cloud, rafforzando ulteriormente il suo vantaggio competitivo.

- Integrazione dei servizi: Google utilizza il suo motore di ricerca come leva per promuovere e integrare i suoi servizi cloud. Ad esempio, molti utenti accedono alle soluzioni cloud di Google (come Google Drive, Google Cloud Platform, ecc.) tramite i servizi già esistenti di Google Search. Questa strategia di integrazione rafforza la dipendenza degli utenti e delle imprese dai servizi di Google, contribuendo al mantenimento della sua posizione dominante.
- Vantaggio competitivo nel digitale: L'infrastruttura digitale di Google è talmente vasta e potente che le permette di fornire servizi cloud a un livello che pochi altri fornitori possono eguagliare. Questo include la possibilità di offrire pacchetti di servizi integrati (motore di ricerca, pubblicità, cloud, intelligenza artificiale), un vantaggio difficile da superare per i concorrenti più piccoli.

Interrogativi fondamentali sulla concorrenza ed equità nel mercato digitale vengono sollevati anche dalla recente accusa di Google nei confronti di Microsoft. Il 25 settembre, Google ha presentato un reclamo alla commissione europea contro Microsoft per pratiche anticoncorrenziali volte a bloccare i clienti sulla piattaforma Azure. In particolare Google sostiene che Microsoft stia sfruttando il suo sistema operativo per impedire la concorrenza, infatti secondo Amit Zavery, vicepresidente di Google Cloud, “Microsoft avrebbe imposto ai suoi clienti un sovrapprezzo del 400% per continuare ad utilizzare Windows Server su piattaforme cloud concorrenti”, invece se avessero continuato ad utilizzare Azure, non avrebbero dovuto sostenere nessun costo aggiuntivo. Zavery afferma inoltre "Stiamo chiedendo alla Commissione Europea di agire ora. Chiediamo loro di considerare davvero questo problema, di aiutare i clienti a decidere e di continuare a offrire loro le scelte”. Infatti secondo Google, Microsoft sta limitando i clienti europei forzandoli ad utilizzare solo il suo ecosistema cloud, nonostante non vi siano impedimenti tecnici all’utilizzo di prodotti della concorrenza. Google cita specificamente il modo in cui Microsoft collega il suo strumento di comunicazione Teams alle sue suite di produttività Office 365 e Microsoft 365, così come le restrizioni imposte ai clienti di Microsoft Azure. Microsoft a sua volta rilancia accusando Google di condurre una “campagna ombra” utilizzando un gruppo chiamato Open Cloud Coalition (OCC) per presentarsi come un sostenitore della concorrenza, ma in realtà il suo fine ultimo sarebbe influenzare le autorità di regolamentazione europee screditando Microsoft ai loro occhi.

1.10 LOCK-IN E SWITCHING COSTS

Diversi fattori contribuiscono alla presenza di costi di switching e al lock-in nel settore del cloud computing, tra questi troviamo:

- Investimenti specifici ed effetti di apprendimento: gli utenti investono tempo e risorse per configurare ed adattare i servizi cloud alle proprie esigenze specifiche, facendo investimenti che non sono facilmente trasferibili ad altri fornitori, un esempio è l'investimento nella formazione dei dipendenti che man mano diventano sempre più familiari con una determinata interfaccia e i servizi di un provider e questa conoscenza non è trasferibile a causa della mancanza di standardizzazione tra le diverse API dei CSP.
- I costi di switching possono essere indotti dai dati. Con l'outsourcing al cloud computing si perde il controllo fisico sui dati, aumenta la difficoltà nell'esportazione e migrazione verso un nuovo fornitore.
- Incompatibilità tecnica tra servizi di diversi fornitori, derivante da implementazioni tecniche differenti o dalla progettazione strategica di servizi proprietari, rende difficile l'interconnessione e può costringere i clienti a dover utilizzare un unico fornitore per l'intero pacchetto di servizi, aumentando i costi di passaggio e rafforzando il lock-in. Infatti molto spesso i CSP implementano *protocolli di sicurezza proprietari*, quali la crittografia dei dati e soluzioni personalizzate che, sebbene efficaci nel proteggere i dati, creano dipendenza da un particolare ecosistema tecnologico.
- Commissioni di uscita (egrees fees) applicate dai fornitori per il trasferimento di dati al di fuori del loro ecosistema, possono aumentare significativamente i costi di passaggio, soprattutto per i clienti con grandi volumi di dati. Queste commissioni possono rendere più costosi anche gli approcci multi-cloud, incentivando ancora una volta l'utilizzo di un unico fornitore e aumentando i costi di passaggio nel lungo periodo.

1.11 CLOUD COMPUTING E INTELLIGENZA ARTIFICIALE

Le applicazioni di intelligenza artificiale richiedono una grande quantità di risorse di calcolo, soprattutto per l'addestramento dei modelli di machine learning. Attualmente stiamo assistendo ad

una crescente domanda di data center, in particolare quelli predisposti per l'intelligenza artificiale. Il cloud computing, come abbiamo visto, è particolarmente utile per gestire i picchi di carico di lavoro, come il cloud bursting il quale permette di eseguire principalmente il carico di lavoro in un ambiente di cloud privato (hosted o in house), ma può espandersi automaticamente su un cloud pubblico per soddisfare picchi improvvisi di domanda, evitando così di dover investire in house in un'infrastruttura hardware sovradimensionata. Attualmente i cosiddetti hyperscaler stanno alimentando gran parte della domanda incrementale di data center AI-ready, per supportare lo sviluppo e l'hosting di modelli di AI di grandi dimensioni, questo è dovuto alla loro esperienza nell'eseguire grandi modelli di AI, come il modello Gemini di Google, o di ospitare modelli creati da altre aziende di IA, come il modello ChatGPT di OpenAI. Il report di McKinsey & Company fornisce una stima della richiesta dei carichi di lavoro AI nei data center in Europa e negli stati uniti ospitati su infrastrutture CSP che si pensa raggiungerà entro il 2030 circa il 60-65% del carico di lavoro totale.

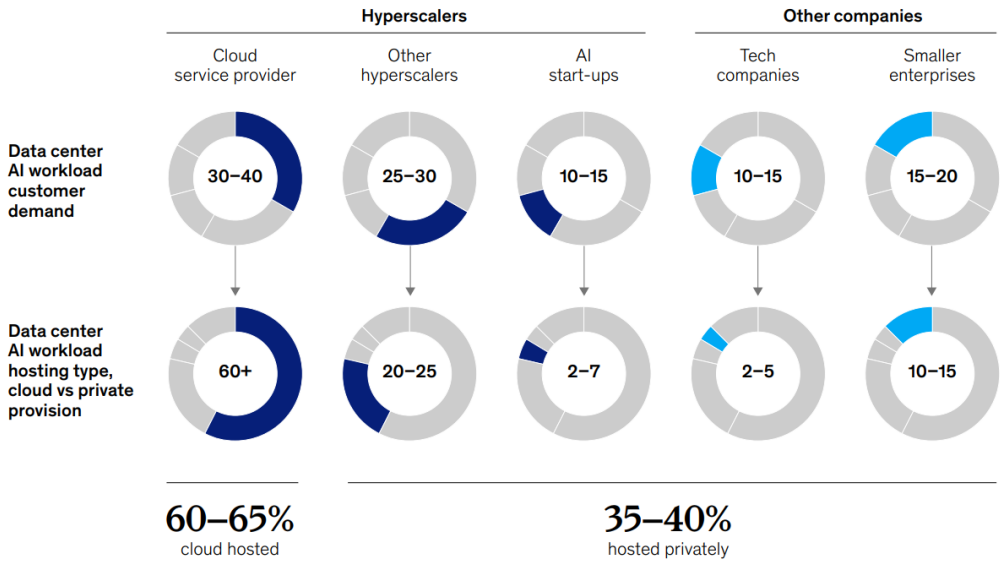

Figure 9: stima della domanda di carichi di lavoro AI tipologia di hosting nei data center in EU e USA nel 2030

Per rispondere alla crescente domanda, i CSP, che attualmente possiedono più della metà della capacità di data center pronti per l'IA a livello mondiale, stanno costruendo rapidamente strutture all'avanguardia. Tuttavia, a causa delle imminenti limitazioni dell'offerta, stanno anche collaborando con provider di colocation (noti come "colo"), ovvero aziende che possiedono e gestiscono data

center, affittando spazio, alimentazione e connettività, che a loro volta stanno espandendo le proprie infrastrutture.

1.12 LA RELAZIONE SIMBIOTICA TRA CLOUD E CYBERSECURITY

Nel panorama digitale moderno, i dati rappresentano il cuore pulsante delle organizzazioni, il successo o il fallimento di un'organizzazione dipendono dalla sua capacità di raccogliere, elaborare e utilizzare le giuste informazioni al momento giusto. Con l'aumento della raccolta di dati nel tempo, sta diventando quasi impossibile archiviare e gestire tutti questi dati fisicamente in sede. Ed è qui che entrano in gioco i fornitori di servizi cloud. Il cloud computing è il pilastro per quanto riguarda l'archiviazione e la gestione. Con il rapido spostamento dei carichi di lavoro verso il cloud e la crescita dello storage cloud e del Software as a Service (SaaS), la sicurezza non è mai stata così cruciale. Le sfide sono molteplici, dalla complessità legata alla protezione dei dati, agli ostacoli di integrazione e alla necessità di stare al passo con un panorama tecnologico in continua evoluzione. Pertanto il cloud computing e la cybersecurity sono due facce della stessa medaglia. La sicurezza diviene quindi un fattore decisivo nella scelta di un'organizzazione di affidarsi ad un provider cloud, poiché le aziende e gli individui affidano ai provider di servizi cloud i propri dati e le proprie applicazioni critiche.

1.13 CYBERSECURITY

"La **Cybersecurity** è il campo dedicato alla protezione dei sistemi informatici, delle reti, dei dati e delle infrastrutture digitali da minacce e attacchi informatici. Queste minacce possono includere virus, malware, attacchi DDoS (Distributed Denial of Service), tentativi di phishing e molti altri tipi di attacchi hacker."

I metodi utilizzati per prevenire, rilevare e rispondere agli attacchi hacker possono essere: crittografia dei dati, oppure monitoraggio delle attività e controlli di accesso di rete e firewall (un sistema di sicurezza che protegge la rete monitorando e controllando il traffico in entrata e in uscita) o ancora software antivirus.

1.14 GLI ELEMENTI DELLA CYBERSECURITY

Le strategie di Cybersecurity si basano sempre su tre principi fondamentali, quali **confidenzialità, integrità e disponibilità** dei dati.

1. Il primo principio della Cybersecurity è la *confidenzialità dei dati*, con il termine confidenzialità in ambito di sicurezza digitale si intende la garanzia che i dati e le informazioni siano preservati dal possibile accesso o utilizzo da parte di soggetti non autorizzati. La confidenzialità va quindi preservata dalla fase di archiviazione a quella di utilizzo e trasmissione delle informazioni.
2. Il secondo principio della Cyber Security è *l'integrità dei dati*. Questo secondo elemento si riferisce alla capacità di non alterare nessun modo il contenuto e il significato da parte di soggetti non autorizzati, mantenendo così l'informazione veritiera.
3. Come terzo e ultimo principio della Cybersecurity troviamo la *disponibilità dei dati*. Quest'ultimo principio si riferisce alla possibilità, per i soggetti autorizzati, di poter accedere alle risorse di cui hanno bisogno in modo ininterrotto. Ciò significa impedire che si verifichi il cosiddetto denial of service e garantire quindi che le risorse infrastrutturali siano pronte per la corretta erogazione del servizio.

Il passaggio dal tradizionale data center locale al cloud comporta una serie di sfide di sicurezza, tra cui:

- **Protezione dei dati**: L'archiviazione dei dati in ambienti cloud, spesso distribuiti su più data center locati in posti diversi, aumenta la superficie di attacco e introduce nuovi minacce. La sicurezza dei dati diventa quindi di fondamentale importanza, richiedendo misure robuste. Il controllo degli accessi e la gestione delle identità assumono un ruolo fondamentale nella prevenzione degli accessi non autorizzati e nella protezione dei dati sensibili, in un contesto in cui la forza lavoro è distribuita e l'accesso alle risorse cloud viene effettuato da remoto.
- **Conformità normativa:** L'adozione del cloud introduce la necessità di conformarsi a una serie di normative e standard di settore relativi alla privacy dei dati e alla protezione dei dati, come il GDPR, HIPAA e PCI DSS. In particolare, alcuni settori come il finanziario o il sanitario,

devono rispettare leggi e normative (ad esempio, il *GDPR*) per proteggere la privacy e la sicurezza dei dati dei clienti.

- **Sicurezza dell'infrastruttura:** I provider di servizi cloud sono responsabili della sicurezza dell'infrastruttura fisica e virtuale sottostante, inclusi server, reti e data center. Le aziende devono valutare attentamente l'attenzione alle tematiche della sicurezza da parte dei provider di cloud, valutando quali sono le loro politiche e le loro procedure di sicurezza per garantire la protezione dei propri dati e applicazioni.
- **Gestione dei rischi di terze parti:** L'adozione del cloud spesso comporta la dipendenza da fornitori di terze parti per una serie di servizi, aumentando la vulnerabilità della catena di approvvigionamento. Le aziende pertanto devono valutare attentamente i rischi associati ai fornitori di terze parti e implementare controlli adeguati per mitigare tali rischi.

Come abbiamo visto il problema della sicurezza è radicato profondamente nel mercato del Cloud computing, ciò ha portato alla nascita di un ramo della cybersecurity che prende il nome di *Cloud Security*.

1.15 CLOUD SECURITY

"Per Cloud Security si intende l'insieme di tecnologie, protocolli e best practice volte a proteggere gli ambienti di Cloud Computing, le applicazioni e i dati in essi contenuti. Si tratta di un ramo della Cybersecurity che si pone come obiettivo primario quello di mantenere sicure e private tutte le informazioni presenti all'interno dell'intera infrastruttura online"

Tra i principi fondamentali della Cloud Security oltre alla protezione dei dati tramite crittografia, e alla gestione delle identità e degli accessi troviamo il Disaster Recovery, la Business Continuity e il DevSecOps (Development, Security and Operations).

La DevSecOps permette ai team di sviluppatori di affrontare i problemi di sicurezza in modo più efficiente. Nei metodi di sviluppo tradizionali i test di sicurezza non facevano parte del ciclo di vita dello sviluppo software (SDLC), pertanto i problemi di sicurezza e le relative falle nel codice venivano scoperte soltanto dopo la creazione del codice. Il framwork DevSecOps migliora questo processo inserendo direttamente nel ciclo di vita dello sviluppo software dei test per rilevare le vulnerabilità.

- I team software non devono attendere il completamento del software per effettuare dei controlli di sicurezza, ma possono eseguirli in ogni fase.
- Ciò porta anche ad una riduzione del time-to-market
- “Creazione di una cultura attenta alla sicurezza” e promozione della consapevolezza: i team di sviluppo diventano più consapevoli in materia di sicurezza poiché è una loro responsabilità assicurarsi che non ci siano falle nel sistema.
- Integrazione continua: “la Continuous Integration and Continuous Delivery (CI/CD)” è una pratica innovativa di sviluppo software che tramite passaggi automatizzati e test permette di effettuare piccole modifiche in risposta ai problemi che vengono individuati dopo il roll out dell’applicazione.

Le conseguenze dei Cyber Attacks non riguardano soltanto gli utenti finali che usufruiscono del servizio di Cloud computing e che subiscono la perdita di dati sensibili per il loro business, ma anche i provider stessi, poiché un attacco informatico intacca la loro reputazione e ciò è dimostrato dalla diminuzione del valore azionario, dell’1.09% circa, che si verifica in media nei tre giorni successivi al cyber attack. La perdita reputazionale, chiamata anche excess loss viene calcolata sottraendo alla perdita totale, registrata sul mercato, i costi diretti legati alla necessità di restaurare il sistema e sopperire al danno causato, infatti i costi legati alla perdita di fiducia dei clienti, il deterioramento delle relazioni commerciali con i partner e il danno alla reputazione non sono quantificabili direttamente. Inoltre la divulgazione di un attacco informatico, ha un impatto negativo anche sul valore azionario dei concorrenti del settore, ciò lascia intendere come gli attacchi rivelino informazioni sensibili sul rischio informatico a livello di settore e non specifiche riguardo all’azienda colpita direttamente. Infine portano a cambiamenti nelle politiche aziendali, infatti le aziende colpite da cyber attacks tendono ad investire maggiormente nella gestione e comprensione dei rischi ad ogni livello della struttura organizzativa e funzionale dell’azienda.

DISASTER RECOVERY

“Il Disaster Recovery è il processo di ripristino dei sistemi informatici e dei dati di un'organizzazione in seguito a un evento catastrofico, naturale come un incendio o un terremoto oppure provocato dall’uomo, come nel caso di un attacco informatico.”

Il disaster recovery insieme alla business continuity fanno riferimento a tutte le misure messe in atto per garantire la continuità del business e un elevato grado di affidabilità. Lo scopo è proprio quello di ridurre al minimo i tempi di inattività.

CAPITOLO 2 – POLICY

2.1 GDPR

La più importante normativa a livello europeo in materia di protezione dei dati, è il regolamento (UE) del parlamento europeo e del consiglio del 27 aprile del 2016 “relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati”. Infatti con il regolamento UE si passa da una visione di possesso del dato, in base alla quale non si può procedere senza il consenso dell’individuo, ad una visione di controllo del dato, che ne sostiene la libera circolazione. Al tempo stesso vengono consolidati i diritti dell'utente, il quale deve essere informato, non soltanto quando i dati vengono utilizzati, ma anche sulle relative modalità d’uso per proteggere lui e l'intera collettività dai rischi impliciti nel trattamento dei dati. Il regolamento pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016 nasce con l’obiettivo principale di creare uno standard comune europeo in materia di protezione dei dati personali. Ciò deriva dal Trattato di Lisbona, grazie al quale la protezione dei dati personali diviene diritto fondamentale degli utenti, pertanto deve essere garantito in tutto il territorio dell’Unione Europea.

Il regolamento introduce diversi diritti, i più rilevanti ai fini dell’analisi sono:

- Diritto di accesso e di informazione ai propri dati personali
- Diritto all’oblio, ovvio diritto alla cancellazione dei dati in determinate circostanze
- Diritto alla portabilità dei dati, ossia il diritto di ottenere i dati in un formato standardizzato in maniera tale che sia possibile trasmetterli ad un altro titolare del trattamento.
- Diritto di recesso in qualsiasi momento
- Diritto di limitazione nel caso si verifichi una violazione del regolamento.

Il regolamento sposta l’attenzione della normativa dalla protezione dell'individuo coinvolto alla responsabilità del titolare e dei responsabili del trattamento.

Vengono riconosciute precise responsabilità in capo al titolare del trattamento dei dati e al responsabile del trattamento, i quali ai sensi dell’articolo 32 (comma 1) “mettono in atto misure

tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono […] la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento e la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico". Tali responsabilità devono essere definite in modo chiaro tramite clausole contrattuali dettagliate.

Il Regolamento Generale sulla Protezione dei Dati (GDPR) trova quindi applicazione anche nel mondo del cloud computing, infatti possiamo identificare le aziende che offrono servizi di cloud computing come responsabili del trattamento dei dati personali dei loro clienti.

Una delle maggiori problematiche relative alla riservatezza è rappresentata dal fenomeno del loss of control, ossia dal rischio che si verifica per l'utente (responsabile del trattamento) con la perdita di controllo sui dati che vengono immessi nel cloud. A ciò si aggiunge anche il rischio che il CSP trasferisca i dati in paesi terzi rispetto all'Unione Europea, a volte anche all'insaputa dell'utente finale.

Nel caso in cui l'utente preveda un possibile trasferimento dei suoi dati all'estero, dovrebbe accertarsi che siano rispettate le norme previste dal CAPO V del GDPR in materia di "*Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali*". Infatti la responsabilità condivisa gli impone di adottare pratiche precauzionali al fine di garantire un adeguato livello di sicurezza per i dati che immette nel cloud computing, ciò si traduce nell'obbligo di valutazione dei documenti contrattuali, del Service Level Agreement e della documentazione in materia di privacy.

Inoltre i provider dei servizi cloud che operano nel territorio dell'Unione Europea, o che trattano dati di cittadini dell'Unione Europea devono:

- Garantire la sicurezza dei dati personali dei loro clienti, lungo ogni fase dell'elaborazione o stoccaggio dei dati, pertanto se i dati personali vengono trasferiti al di fuori dell'UE i provider devono garantire la compliance regolatoria
- La liceità del Trattamento: Le aziende di cloud computing devono avere una base legale per il trattamento dei dati personali dei loro clienti, come il consenso, un contratto o un obbligo legale. Possono stipulare diversi tipi di contratti in base al servizio offerto

    - Appalto di servizi: prevede l'obbligo per il fornitore di svolgere un'attività in favore del cliente dietro un corrispettivo, viene utilizzato per servizi come l'hosting o il backup che non richiedono un livello di personalizzazione del servizio
    - Contratto di somministrazione, si utilizza nel caso di fornitura periodica o continuativa di beni o servizi
    - Contratto di licenza, stabilisce le modalità di utilizzo del servizio con limitazioni sulla redistribuzione e vincoli tecnici imposti all'utente.
    - Contratto di "locazione", viene utilizzato nel caso di Infrastructure as a Service) e (Platform as a Service), poiché in questi casi il provider controlla le risorse, ma l'utente ha piena libertà di utilizzo
- Trasparenza e Informazione: Le aziende di cloud computing devono essere trasparenti con i loro clienti sul modo in cui trattano i dati personali. Devono fornire informazioni chiare e concise sull'identità del titolare del trattamento, le finalità del trattamento, i destinatari dei dati e i diritti dell'interessato.
- I diritti dell'Interessato: Le aziende di cloud computing devono garantire ai loro clienti l'esercizio dei loro diritti ai sensi del GDPR, come il diritto di accesso, rettifica, cancellazione e portabilità dei dati.

Il GDPR introduce inoltre la figura del responsabile della protezione dei dati (DPO), per i provider di una certa dimensione o che trattano dati particolari. Il DPO ha il compito di assistere l'azienda nell'applicazione del GDPR e di garantire la protezione dei dati personali.

Il regolamento prevede inoltre l'istituzione di autorità di controllo indipendenti in ogni stato membro, che devono garantire la corretta applicazione dello stesso, viene introdotto anche un meccanismo di coerenza per garantire uniformità nell'applicazione all'interno dell'unione ed infine sono previste delle sanzioni in caso di violazione delle disposizioni.

All'interno del quadro più ampio del Digital Strategy dell'UE per garantire un'economia digitale equa, competitiva e rispettosa dei diritti dei cittadini e delle imprese troviamo oltre al GDPR anche il Data Act.

2.2 DATA ACT

Il Data Act, ovvero il "Regolamento del Parlamento Europeo e del Consiglio sulle norme armonizzate in materia di accesso e utilizzo equi dei dati", emanato il 13 dicembre 2023, rappresenta una pietra miliare nella regolamentazione del mercato del Cloud Computing. Il Data Act, si applica in generale ai Digital Processing Service (DPS) definiti all'articolo 2 "servizio di trattamento dei dati: un servizio digitale fornito a un cliente e che consente l'accesso di rete universale e su richiesta a un pool condiviso di risorse informatiche configurabili, scalabili ed elastiche di natura centralizzata, distribuita o altamente distribuita e che può essere rapidamente erogato e rilasciato con un minimo sforzo di gestione o interazione con il fornitore di servizi".

Il Data Act è una legge ideata per migliorare l'economia dei dati dell'UE, promuovere la competizione e incoraggiare allo stesso tempo l'innovazione. Entrerà in vigore il 12 settembre 2025 con l'obiettivo di rendere la concorrenza nel mercato europeo più equa. La commissione europea si impegna a stilare una serie di clausole contrattuali standard da utilizzare per i contratti tra i fornitori e gli utenti, che "aumentano la fiducia nei servizi di elaborazione dati, creano una relazione più equilibrata tra utenti e fornitori di servizi di elaborazione dati e migliorano la certezza del diritto per quanto riguarda le condizioni che si applicano per il passaggio ad altri servizi di elaborazione dati."

Gli obiettivi del Data Act sono:

- Abbassare le barriere all'ingresso di nuovi fornitori nel mercato del cloud computing, eliminando ostacoli pre-commerciali, commerciali, tecnici, contrattuali e organizzativi.
- Rendere i clienti meno dipendenti dal singolo provider (sia per i servizi B2B sia per quelli B2C), permettendo così ai clienti di utilizzare servizi da diversi fornitori
- Rendere più fluido e veloce il passaggio da un provider ad un altro senza interruzioni di servizio o perdita di dati ed informazioni.

L'ultimo punto viene trattato nel Capo VI del Data Act in particolare nell'articolo 25, nel quale vengono descritte le condizioni necessarie affinché si possa rescindere un contratto e stipularne un altro con un nuovo provider.

Articolo 25 “Termini contrattuali relativi al passaggio di consegne”

“I diritti del cliente e gli obblighi del fornitore di servizi di elaborazione dati in relazione al passaggio tra fornitori di tali servizi o, ove applicabile, a un'infrastruttura ICT in sede devono essere chiaramente stabiliti in un contratto scritto. Il fornitore di servizi di elaborazione dati deve rendere tale contratto disponibile al cliente prima della firma del contratto in modo tale da consentirgli di archiviare e riprodurre il contratto.”

Inoltre viene stabilito che il provider debba

“fornire ragionevole assistenza al cliente e a terzi autorizzati dal cliente nel processo di cambio […] agire con la dovuta diligenza per mantenere la continuità aziendale e continuare a fornire le funzioni o i servizi previsti dal contratto […] garantire che venga mantenuto un elevato livello di sicurezza durante l'intero processo di trasferimento, in particolare la sicurezza dei dati durante il loro trasferimento e la sicurezza continua dei dati durante il periodo di recupero specificato”.

Si stabilisce quindi

“l'obbligo del fornitore di servizi di elaborazione dati di supportare la strategia di uscita del cliente in relazione ai servizi contrattuali, anche fornendo tutte le informazioni pertinenti”.

Vengono definiti anche altri obblighi contrattuali ai quali il provider deve ottemperare

- Garantire un periodo transitorio per il passaggio di 30 giorni
- Garantire un periodo di preavviso per l’avvio del processo di cambio,
- Includere nel contratto una clausola che garantisca la cancellazione di tutti i dati esportati dal cliente a seguito del passaggio alla scadenza del periodo di recupero prestabilito.
- Il provider deve inoltre fornire informazioni chiare sui rischi riguardanti le possibili interruzioni durante il periodo di passaggio e sulla tipologia di dati e risorse digitali che possono essere trasferite.
- I fornitori di origine e destinazione “devono collaborare in buona fede per rendere efficace il processo di passaggio, consentire il trasferimento sicuro e tempestivo dei dati necessari in

un formato comunemente utilizzato e leggibile da una macchina e mediante interfacce aperte, evitando al contempo interruzioni del servizio e mantenendo la continuità del servizio." (Articolo 23, paragrafo 2)

- Gradualmente verranno ritirate le spese di switching a partire dal 12 gennaio 2027, fino ad una completa eliminazione dei suddetti costi se non quelli strettamente necessari per coprire le spese in cui incorre il provider per effettuare il passaggio (Articolo 29). Inoltre, è importante per garantire "l'implementazione di successo di strategie multi-cloud, che consentono ai clienti di implementare strategie ICT a prova di futuro e che riducono la dipendenza dai singoli fornitori di servizi di elaborazione dati." (Considerando 80)
- Le tariffe per effettuare la migrazione vanno inserite nel contratto, soprattutto nel caso in cui si parli di un passaggio altamente complesso o costoso

Il Data Act introduce il concetto di "funzionalità equivalenti", riguardanti servizi come l'Iaas. Questo concetto mira a garantire che i clienti possano ripristinare un livello minimo di funzionalità del servizio presso il nuovo fornitore, senza comprometterne l'operabilità. Inoltre, il Data Act promuove l'unbundling dei componenti dei servizi infrastrutturali, in modo tale che i clienti abbiano la possibilità di scegliere e di utilizzare solo i servizi specifici di cui hanno bisogno, combinando eventualmente anche soluzioni da fornitori diversi.

Gli obblighi riguardanti le procedure di passaggio e trasferimento dei dati, come anche la struttura e i formati dei dati e le norme di interoperabilità più precisamente prendono il nome di obblighi informativi. Sono previste inoltre sanzioni, multe e avvertimenti nel caso in cui il provider non adempia a qualcuno dei suddetti obblighi.

Vediamo subito come la volontà sia quella di costruire e rafforzare l'interoperabilità tra i diversi provider cloud puntando alla riduzione, se non ad annullare, tutti i costi di switching e le difficoltà legate al passaggio, come viene definito nel Considerando 81 "La capacità dei clienti dei servizi di elaborazione dati, inclusi i servizi cloud e edge, di passare da un servizio di elaborazione dati a un altro mantenendo una funzionalità minima del servizio e senza tempi di inattività, o di utilizzare contemporaneamente i servizi di più fornitori senza ostacoli indebiti e senza costi di trasferimento dei dati, è una condizione fondamentale per un mercato più competitivo, con barriere d'ingresso

più basse per i nuovi fornitori di servizi di elaborazione dati, e per garantire una maggiore resilienza per gli utenti di tali servizi. Anche i clienti che beneficiano di offerte gratuite dovrebbero beneficiare delle disposizioni per il passaggio previste da questo regolamento, in modo che tali offerte non determinino una situazione di lock-in per i clienti."

Il fine ultimo del Data Act è quello di promuovere l'innovazione aperta e la crescita economica nell'unione europea.

Ciò si evince anche dall'impegno e l'interesse che l'UE sta riponendo nei confronti dell'Edge computing, infatti nel Considerando 80 troviamo "Il calcolo edge, che rappresenta una forma di elaborazione dati altamente distribuita, è previsto possa generare nuovi modelli di business e modelli di erogazione di servizi cloud, che dovrebbero essere aperti e interoperabili sin dall'inizio."

Questo riflette pienamente lo spirito e la direzione intrapresa nella Strategia Europea per i Dati, la quale evidenzia l'importanza dell'edge computing come strumento chiave per il futuro dell'infrastruttura digitale europea, che punta alla creazione di spazi europei comuni per i dati. Inoltre l'UE può svolgere un ruolo chiave nella definizione di standard di interoperabilità garantendo la portabilità dei dati e la compatibilità tra diverse soluzioni, questa rappresenta la sfida più grande sia a livello europeo sia a livello mondiale. Inoltre la mancanza di standard condivisi e la grande frammentazione dell'edge computing comportano problemi di gestione dell'infrastruttura stessa.

Gli elementi che maggiormente contribuiscono alla diffusione dell'edge computing sono la bassa latenza infatti, grazie alla possibilità di elaborare i dati localmente, l'edge computing riesce a ridurre al minimo i tempi di trasferimento dei dati e di risposta, migliorando così il funzionamento delle applicazioni in tempo reale come i sistemi di guida autonoma (ADAS) e la realtà aumentata. Inoltre la possibilità di elaborare i dati localmente riduce la dipendenza dalla rete internet e migliora il tasso di affidabilità dei sistemi, soprattutto nel caso di applicazioni critiche, riducendo così anche i rischi e i costi (di banda e di rete) associati al trasferimento, dato che l'elaborazione e l'archiviazione avvengono in locale.

L'implementazione è abbastanza costosa, così come la manutenzione, poiché i siti di edge computing sono spesso situati in aree remote, ciò rende più difficili l'accesso per il personale tecnico

specializzato. Inoltre i dati generati devono essere protetti da minacce, e da attacchi malevoli, il che risulta particolarmente complesso considerando che questi dati sono distribuiti in diverse aree remote, lontane dal perimetro di sicurezza dell'azienda stessa, pertanto l'aspetto della sicurezza è centrale anche in un contesto diverso come quello dell'edge computing.

Il Data Act inoltre stabilisce anche delle norme per garantire la sicurezza dei dati nel mondo cloud, l'articolo 102 riguarda la sicurezza dei dati "Per promuovere una maggiore fiducia nei dati, è importante che vengano implementate, nella misura del possibile, misure di salvaguardia per garantire il controllo dei propri dati da parte dei cittadini dell'Unione, degli enti pubblici e delle imprese. Inoltre, dovrebbero essere rispettati il diritto, i valori e gli standard dell'Unione riguardanti, tra l'altro, la sicurezza, la protezione dei dati e la privacy e la tutela dei consumatori."

Il Data Act non è l'unico tentativo di regolamentare il mercato del cloud computing, infatti nel 2022 l'Unione Europea ha emanato il Digital Market Act (Regolamento (UE) 2022/1925).

2.3 DIGITAL MARKET ACT

Il DMA si concentra sui "Core Platform Services" (CPS), un elenco di servizi digitali considerati cruciali per l'economia digitale, tra cui i servizi di Cloud Computing e si applica solo alle imprese che si qualificano come "gatekeeper" per un determinato CPS. In particolare, il DMA definisce come gatekeeper un'impresa che soddisfa tre criteri qualitativi generali

Articolo 3

"(a) ha un impatto significativo sul mercato interno; (b) fornisce un servizio di piattaforma di base che costituisce un punto di accesso (gateway) importante affinché gli utenti commerciali raggiungano gli utenti finali; e c) detiene una posizione consolidata e duratura, nell'ambito delle proprie attività, o è prevedibile che acquisisca siffatta posizione nel prossimo futuro."

Il DMA (Digital Markets Act) identifica anche delle soglie quantitative, in modo tale da rendere univoca l'identificazione del gatekeeper

- Fornitura del CSP in almeno tre Stati membri dell'Unione,

- Negli ultimi tre esercizi finanziari, il fatturato annuo globale realizzato nell'esercizio finanziario precedente nell'Unione Europea pari o superiore a 7,5 miliardi di euro, oppure la capitalizzazione di mercato media nell'ultimo esercizio finanziario pari o superiore a 65 miliardi di euro.
- Negli ultimi tre esercizi finanziari, almeno 45 milioni di utenti finali mensili mediamente attivi stabiliti o ubicati nell'Unione e almeno 10.000 utenti aziendali annualmente attivi stabiliti nell'Unione.

L'attività di identificazione dei gatekeeper è affidata esclusivamente alla Commissione, il processo di designazione è basato su un'analisi caso per caso e deve tenere conto delle caratteristiche specifiche di ciascun CSP e del mercato in cui opera. Inoltre viene rivisto almeno ogni tre anni, anche sulla base delle notifiche che i fornitori di servizi di piattaforma principale sono obbligati a fare se raggiungono le soglie quantitative. Pertanto il superamento delle soglie quantitative non implica automaticamente la designazione di gatekeeper, la decisione ultima spetta alla commissione Europea.

Questo rende il DMA una regolamentazione *asimmetrica e orizzontale*:

- Asimmetrica perché non si applica a tutte le aziende del settore digitale, ma soltanto alle aziende che rispondono a specifici criteri, ovvero quelle che sono considerate "gatekeeper", le quali hanno una posizione dominante e sono capaci di influenzare la competizione nel mercato, pertanto è essenziale che vengano regolamentare poiché i loro comportamenti possono causare danni alla concorrenza e ai consumatori
- Viene definita una regolamentazione orizzontale perché impone gli stessi obblighi ad aziende appartenenti a settori diversi con modelli di business differenti. Infatti le stesse regole vengono applicate a piattaforme di social media, motori di ricerca, cloud provider e così via.

Questa combinazione potrebbe non rivelarsi ottimale in quanto risulta difficile imporre le stesse regole a mercati diversi nei quali i requisiti di equità e competitività sono differenti tra di loro. Pertanto, la sfida è trovare regole armonizzate che funzionino bene in un contesto così variegato.

La volontà di racchiudere in un'unica regolamentazione tutte le piattaforme digitali, fa sì che le soglie e gli obblighi definiti in essa non siano sempre aderenti al 100% a tutti le tipologie di CCS.

Dalla descrizione dei requisiti sia qualitativi che quantitativi per l'individuazione di un gatekeeper vediamo subito che i fornitori di servizi cloud presentano alcune peculiarità rispetto ad altri CSP. Di solito, i Core Platform Services (come i social media o i motori di ricerca) hanno una struttura bilaterale (o multisided), cioè collegano due gruppi di utenti: gli utenti commerciali (come le aziende) e gli utenti finali (i consumatori). In questi casi, le piattaforme funzionano come intermediari che facilitano il contatto tra aziende e consumatori. I CCS, invece, sono unilaterali, cioè non svolgono il ruolo di intermediazione tra due gruppi diversi di utenti e quindi non agiscono da "gateway" che collega utenti commerciali con utenti finali, piuttosto il ruolo del Cloud Service Provider è quello di offrire risorse di calcolo (come spazio di archiviazione e potenza di calcolo) ad utenti aziendali. Quindi manca una caratteristica fondamentale per definire un CSP come gatekeeper secondo il DMA e di conseguenza per poter applicare gli obblighi previsti dal DMA negli articoli 5 e 6, entrambi parte del Capo III **"**Practices of Gatekeepers that limit contestability or are unfair"

Articolo 5 "Obligations for gatekeepers"

L'Articolo 5 del Digital Markets Act (DMA) stabilisce una serie di obblighi per i gatekeeper per garantire mercati equi e contendibili ed evitare che abusino della loro posizione dominante. A differenza degli obblighi dell'articolo 6 non richiedono ulteriori specifiche da parte della commissione europea, pertanto l'applicazione deve essere diretta e immediata da parte dei Gatekeeper a ciascuno dei loro servizi di piattaforma di base.

Alcuni obblighi previsti dall'articolo 5 sono:

- Limitazioni sull'uso dei Dati Personali, ad esempio i gatekeeper non possono utilizzare i dati personali raccolti da terzi che utilizzano i suoi servizi di piattaforma per la pubblicità online, non possono combinare i dati provenienti da un servizio con dati provenienti da un altro servizio o con dati di terzi.

- I gatekeeper non possono impedire agli utenti commerciali di commercializzare e pubblicizzare i loro prodotti o servizi ai fruitori finali senza costi aggiuntivi.
- Deve essere garantita la libertà di offrire prezzi diversi su altri canali
- Libertà di Sollevare Questioni Legali, i gatekeeper hanno l'obbligo di consentire agli utenti finali di segnalare alle autorità eventuali problemi di non conformità. Pertanto I gatekeeper non possono impedire né limitare la possibilità per utenti commerciali e finali di sollevare questioni legali contro il gatekeeper in caso di violazioni delle leggi nazionali o dell'UE.
- Libertà di scegliere servizi tecnici di terzi
- Divieto di abbonamenti forzati: I gatekeeper non possono costringere gli utenti o le aziende a iscriversi ad altri servizi della loro piattaforma come condizione per accedere ai servizi principali.

Articolo 6 "Obligations for gatekeepers susceptible of being further specified"

Anche qui, troviamo diversi obblighi, alcuni dei quali non strettamente applicabili al mondo del cloud computing, come il divieto di utilizzo dei dati non pubblici degli utenti commerciali per competere questi ultimi oppure "Il gatekeeper non garantisce un trattamento più favorevole, in termini di posizionamento e relativi indicizzazione e crawling, ai servizi e prodotti offerti dal gatekeeper stesso rispetto a servizi o prodotti analoghi di terzi. Il gatekeeper applica condizioni trasparenti, eque e non discriminatorie a tale posizionamento."

Gli obblighi aderenti al contesto competitivo del cloud computing sono i seguenti:

- I gatekeeper non possono impedire agli utenti finali di accedere a servizi o applicazioni di terzi sui loro dispositivi o sistemi operativi. Questo obbligo mira a promuovere la libertà di scelta per gli utenti finali e a prevenire che i gatekeeper li vincolino a utilizzare i propri dispositivi o sistemi operativi.
- Il gatekeeper deve garantire l'effettiva interoperabilità, a titolo gratuito, per fornitori di servizi e hardware: I gatekeeper devono consentire l'interoperabilità gratuita con le proprie componenti hardware e software per i fornitori di servizi e hardware di terzi, oltre che per i

servizi forniti contestualmente alla piattaforma di base. Tuttavia, possono implementare misure necessarie per garantire l'integrità del sistema.

- Obbligo di informare gli utenti commerciali delle modifiche alle condizioni di accesso al CPS con congruo preavviso: I gatekeeper sono tenuti a informare gli utenti commerciali di qualsiasi modifica sostanziale alle condizioni di accesso al CPS con un preavviso di almeno 15 giorni. Questo obbligo mira a dare agli utenti commerciali il tempo sufficiente per adattarsi alle nuove condizioni o per cercare alternative, prevenendo che i gatekeeper introducano modifiche improvvise e dannose per i loro interessi.
- Obbligo di garantire una portabilità dei dati efficace, in tempo reale e gratuita per gli utenti finali: simile all'obbligo dell'articolo 5, questo punto specifica che la portabilità dei dati deve essere efficace, in tempo reale e gratuita per gli utenti finali. Ciò significa che i gatekeeper devono fornire agli utenti finali la possibilità di trasferire i propri dati in modo semplice, rapido e senza costi aggiuntivi. L'obiettivo è di ridurre l'effetto di lock-in e a facilitare il passaggio degli utenti finali a servizi concorrenti.
- Obbligo di garantire l'accesso ai dati/portabilità in tempo reale e gratuita per gli utenti business ai dati associati ai loro servizi: questo comma precisa che l'accesso ai dati per gli utenti business deve essere in tempo reale e gratuito. Ciò significa che i gatekeeper devono fornire agli utenti business la possibilità di accedere e trasferire i propri dati in modo semplice, rapido e senza costi aggiuntivi.
- Obbligo di consentire agli utenti commerciali di utilizzare servizi di terzi per la verifica dell'identità degli utenti finali: I gatekeeper non possono obbligare gli utenti commerciali a utilizzare esclusivamente il proprio sistema di identificazione per la verifica dell'identità degli utenti finali. Devono consentire l'utilizzo di sistemi di identificazione di terze parti, a condizione che questi sistemi siano conformi agli standard di sicurezza e privacy pertinenti.
- Divieto di imporre condizioni sproporzionate per la cessazione dei servizi: I gatekeeper non possono rendere difficile o costoso per gli utenti commerciali la cessazione dei loro contratti o la disattivazione dei loro account. Le condizioni di cessazione devono essere chiare, trasparenti e non discriminatorie. L'obiettivo è di proteggere gli utenti business e a prevenire che i gatekeeper rendano difficile o costoso il passaggio a servizi concorrenti.

Una possibile interpretazione dei CSP come gateway potrebbe essere quella secondo la quale rappresentano un'infrastruttura essenziale per molte aziende affinché possano commercializzare i loro prodotti, in questo senso il provider può essere visto come un gateway essenziale, ma ciò comunque non implica necessariamente l'esistenza di un mercato bidirezionale. Microsoft sostiene "Tendiamo a usare il termine "piattaforma" indiscriminatamente nel linguaggio quotidiano per riferirci a un'ampia varietà di tecnologie. Tuttavia, non tutte le "piattaforme" sono o possono essere gatekeeper; molte sono semplicemente servizi che le aziende utilizzano per funzionare e operare. Ad esempio, le aziende possono utilizzare servizi di cloud computing (il cloud pubblico) per ospitare il loro sito Web, creare un'app per le spese dei loro dipendenti, monitorare le informazioni dei clienti o analizzare i dati di vendita." Ciò implica che la definizione stessa di business user e end user nel mondo del cloud computing non sia sempre chiara e definita, proprio perché non è sempre facile assimilare il concetto di piattaforma bilaterale al mercato del cloud computing.

L'ambiguità presente nel DMA riguardo il mercato del cloud computing si estende anche agli obblighi ai quali sono soggette le aziende considerate come Gatekeeper, infatti alcuni obblighi previsti dal DMA e riguardanti la condivisione dei dati (soprattutto per i motori di ricerca e le piattaforme pubblicitarie), sembrano non applicabili ai servizi di cloud computing, in particolare l'Iaas, Microsoft contesta questa scelta sostenendo che "il divieto di condividere i dati degli utenti finali tra i servizi di piattaforma ha senso per quei servizi che monetizzano direttamente tali dati vendendo pubblicità basata su di essi. Ma comprometterà la qualità e l'innovazione per quei servizi di piattaforma che utilizzano tali dati solo per fornire migliori protezioni di sicurezza e un'esperienza utente coerente tra di essi." Invece altri obblighi, come la portabilità dei dati e la rimozione degli ostacoli allo switching, sono fondamentali per garantire la concorrenza nel cloud computing.

Questo deriva anche dalla complessità nella definizione del mercato del cloud computing, data dalla presenza di diversi modelli di servizio e di deployment che rende arduo determinare quali prodotti e servizi siano considerati sostituti dai clienti, pertanto risulta quasi impossibile regolamentarli in un'unica definizione onnicomprensiva.

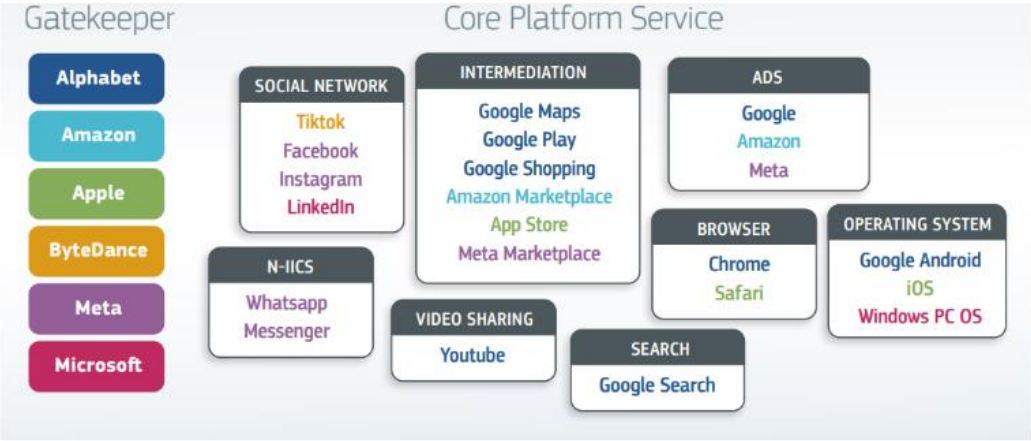

Figure 10: Designazione dei Gatekeeper e i relativi Core Platform Service

L'Unione Europea ha designato alcuni gatekeeper e i relativi "Core Platform Service" per i quali sono state designata come gatekeeper. Come possiamo osservare non è stato designato nessun servizio Cloud, nonostante secondo uno studio commissionato dal Cispe, realizzato da Frederic Jenny (presidente della commissione concorrenza dell'Ocse) condotto fra 25 aziende che usano servizi di cloud computing in Europa abbiano denunciato "condizioni di mercato sleali imposte dalle grandi aziende del software per l'accesso alla loro infrastruttura cloud tecniche di pricing vessatorie e difficoltà nel passaggio a un fornitore concorrente. Inoltre le imprese hanno segnalato anche che "molti fornitori del cloud vendono insieme all'accesso all'infrastruttura anche i loro prodotti software in un unico pacchetto in modo da rendere meno attraenti o convenienti i prodotti della concorrenza."

Pertanto vediamo come il DMA riconosca che la combinazione di grandi economie di scala, effetti di rete diretti e indiretti e vantaggi basati sui dati creino mercati altamente concentrati, in cui poche aziende, definite come gatekeeper hanno una posizione dominante capace di influenzare le dinamiche competitive danneggiando i consumatori e l'equità nelle relazioni commerciali tra le imprese che forniscono tali servizi e i loro utenti aziendali e finali. Si propone di prevenire effetti di lock-in e mancanza di multihoming, condizioni necessarie per abbattere barriere all'ingresso e permettere l'entrata di nuovi provider. Allo stesso tempo il DMA è stato aspramente criticato, anche per la difficoltà implementativa e di monitoraggio soprattutto delle aziende globali e per la poca specificità che potrebbe comprometterne l'applicabilità, questa rappresenta una sfida per la Commissione Europea che dovrà garantire un'applicazione efficace del DMA ai CCS.

2.4 CYBERSERCURITY ACT

Il REGOLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 17 aprile 2019 "relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione"

Il regolamento sulla Cybersicurezza si propone di migliorare il livello di cybersicurezza nell'Unione Europea, promuovendo la cooperazione tra gli Stati membri e definendo un quadro per la certificazione della cybersicurezza degli ICT services (Information and Communication Technology services) "servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo della rete e dei sistemi informativi", dei processi e prodotti ICT, definiti rispettivamente come "un insieme di attività svolte per progettare, sviluppare, fornire o mantenere un prodotto TIC o servizio TIC" e "un elemento o un gruppo di elementi di una rete o di un sistema informativo".

L'ENISA (Agenzia dell'Unione Europea per la cibersicurezza), rappresenta il fulcro in merito agli aspetti della cybersecurity supportando le organizzazioni, gli stati membri, il settore pubblico e qualsiasi stakeholder nella protezione delle reti e dei sistemi informativi, migliorandone la resilienza e le tempistiche di risposta agli attacchi informatici. Inoltre l'ENISA mira a raggiungere un approccio armonizzato all'interno dell'Unione Europea, promuovendo "l'uso della certificazione europea della cibersicurezza, con l'obiettivo di evitare la frammentazione del mercato interno." (Articolo 4.6)

Affronta quindi la necessità di un approccio armonizzato alla certificazione della sicurezza informatica in modo da ottenere un livello comune ed elevato di cybersecurity.

Gli obiettivi principali di questo regolamento sono:

- Rafforzare la *fiducia* nelle tecnologie digitali: vista la crescente digitalizzazione, la sicurezza informatica è essenziale per garantire la fiducia da parte dei clienti (aziende, pubbliche amministrazioni e privati) pertanto il regolamento mira a proteggere le reti, i sistemi informativi e i servizi digitali in modo da ridurre il rischio di un attacco malevolo.

- Migliorare la resilienza dell'UE agli attacchi informatici, cercando di rafforzare la sicurezza informatica a livello dell'Unione Europea a fronte di un panorama in cui le minacce informatiche sono in continua evoluzione, è necessario migliorare la capacità di risposta a qualsiasi tipologia di cyber hattack
- Promuovere un mercato unico digitale per la cybersecurity promuovendo l'uso della certificazione europea, ma anche "la cooperazione, inclusa la condivisione di informazioni, e il coordinamento a livello di Unione tra gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione e i portatori di interessi del settore pubblico e privato su questioni relative alla cibersicurezza." (articolo 4.4)
- Riduzione della dipendenza da fornitori esterni, il Cybersecurity Act mira a promuovere una maggiore autonomia strategica dell'UE nel settore del cloud computing, riducendo la dipendenza dai grandi fornitori extraeuropei. Questo è particolarmente importante sia per proteggere dati delle infrastrutture critiche, come sanità ed energia, ma anche per garantire che gli standard di sicurezza Europei.

Con l'adozione del Cybersecurity Act, nel 2019, l'ENISA è stata incaricata di creare schemi di certificazione per migliorare la sicurezza informatica nell'UE, inclusi i servizi di cloud.

La certificazione copre aspetti come:

- Sicurezza dei dati: protezione contro accessi non autorizzati e perdita di dati.
- Continuità del servizio: garanzie di uptime e recupero rapido in caso di incidenti.
- Conformità con normative europee, come il GDPR.

Il cybersecurity act è destinato ad avere un impatto determinante sul settore del cloud computing, infatti standard europei sulla sicurezza contribuiscono ad aumentare la fiducia degli utenti, in quanto avranno la possibilità di scegliere servizi cloud che li rispettano, ciò contribuirà alla competizione delle aziende europee a livello mondiale.

Uno degli schemi principali per la certificazione nell'ambito del cloud computing previsti dal Cybersecurity Act, sviluppato dall'ENISA è l'EUCS (EU Cloud Security Scheme).

2.4.1 EUCS

L'EUCS si propone di fornire:

- Standard di sicurezza comuni: creare una base uniforme di requisiti di sicurezza per i servizi cloud utilizzati in tutta l'UE, riducendo le disparità tra i vari standard nazionali, in modo da facilitare anche la comparabilità tra i servizi cosicché gli utenti possano confrontare i servizi cloud in base ai livelli di sicurezza offerti.
- Aumentare la Fiducia e la Trasparenza: dare a clienti e aziende europee la sicurezza che i servizi cloud certificati rispettino livelli di protezione definiti e verificabili. Infatti sapendo che un servizio cloud è certificato secondo standard di sicurezza riconosciuti dall'UE, aziende e pubbliche amministrazioni possono fare affidamento su servizi cloud sicuri e conformi.

Il progetto è uno schema volontario che possa essere applicato ad ogni servizio cloud. L'obiettivo è quello di garantire che i provider rispettino standard elevati di sicurezza offrendo ai clienti dell'UE maggiori garanzie sulla protezione dei dati e sulla conformità alle normative. Sono previsti diversi livelli di sicurezza (Basic, Substantial e High) che i fornitori di servizi cloud devono soddisfare a seconda del contesto e delle esigenze di sicurezza dei clienti.

- Livello base di sicurezza, adatto a servizi che non gestiscono dati sensibili o critici. Comprende requisiti di sicurezza essenziali.
- Livello intermedio (Substantial) indicato per servizi che trattano dati sensibili e richiedono maggiori misure di sicurezza. I controlli sono più rigorosi rispetto al livello base.
- High, livello elevato di sicurezza, destinato a servizi che gestiscono dati altamente sensibili o critici per l'operatività e la sicurezza di infrastrutture strategiche. Questo livello richiede controlli di sicurezza avanzati e prevede standard di protezione molto stringenti.

Il processo di certificazione EUCS prevede diverse fasi che variano in base al livello di affidabilità desiderato e alla tipologia di prodotto, servizio o processo ICT. La fase più importante è quella relativa alla valutazione della conformità. Il provider può scegliere tra due modalità:

- Valutazione da parte di un organismo terzo della conformità

- Autocertificazione

La seconda modalità viene utilizzata per prodotti a basso rischio e il livello di affidabilità è “basic”. Invece la certificazione da parte di un organismo terzo accreditato dall’autorità nazionale, è il metodo stardard utilizzato dai provider per testimoniare la sicurezza informatica di sistemi atti all’elaborazione di carichi di lavoro critici per l’utente.

Le regole per la designazione di una o più Autorità Nazionale di Certificazione della Cibersicurezza (ANCC) vengono stabilite **nell’articolo 58** del regolamento sulla Cybersicurezza, che si concentra sul ruolo chiave svolto da queste autorità nell’attuazione del quadro europeo di certificazione della sicurezza informatica.

Le Autorità Nazionali di Certificazione della Cibersicurezza sono responsabili della supervisione e del controllo della conformità per i certificati di cybersicurezza rilasciati all'interno dei confini nazionali, garantendo che i prodotti e servizi TIC (Tecnologie dell'Informazione e della Comunicazione) rispettino i requisiti di sicurezza.

L’iter di designazione delle autorità di certificazione prevede che dopo la nomina da parte di ogni stato membro di una o più ANCC, ne venga comunicata l’identità alla Commissione Europea specificando i compiti di ognuna di esse. Le autorità inoltre devono operare in modo indipendente in ogni aspetto (strutturale, finanziario e organizzativo) dai soggetti sui quali vigilano. Questa indipendenza è fondamentale per garantire l'imparzialità e l'integrità del processo di certificazione. Inoltre gli stati membri devono garantire risorse sufficienti alle ANCC per svolgere in maniera adeguata il loro ruolo di vigilanza e certificazione, infine devono far parte dell’European Cybersecurity Certification Group (ECCG).

L’ECCG è costituito da figure rappresentative delle autorità nazionali di certificazione della sicurezza e assiste la commissione europea nell’attuazione e applicazione del quadro di certificazione.

Per garantire l’armonizzazione a livello europeo, **l’articolo 59** prevede una “Valutazione inter pares”

"Al fine di ottenere norme equivalenti in tutta l'Unione relativamente ai certificati europei di cibersicurezza e alle dichiarazioni UE di conformità, le autorità nazionali di certificazione della cibersicurezza sono soggette a una valutazione inter pares."

2.4.2 NIS2

Oltre all'EUCS, anche la direttiva NIS2 è stata sviluppata per creare un livello di sicurezza informatica comune elevato tra gli Stati membri, tale direttiva è entrata nel diritto nazionale degli stati membri, in data 17 ottobre 2024.

La direttiva introduce una classificazione dei soggetti in due categorie principali:

- Soggetti essenziali: sono coloro la cui interruzione operativa avrebbe un impatto significativo sulla fornitura di servizi critici per la società e l'economia, tra i quali rientrano i cloud provider.
- Soggetti importanti, svolgono comunque un ruolo rilevante e l'interruzione del loro servizio avrebbe un impatto negativo, ma meno drastico rispetto a quello dei soggetti essenziali.

La classificazione in soggetti essenziali e soggetti importanti determina l'intensità degli obblighi di sicurezza informatica e la severità delle sanzioni.

Sia i soggetti essenziali sia i soggetti importanti sono tenuti ad adottare misure di gestione dei rischi di cibersicurezza. Tuttavia, la direttiva prevede una maggiore specificità nelle misure da adottare per i soggetti essenziali. Entrambi sono tenuti a segnalare incidenti significativi. Ed infine la direttiva impone delle sanzioni, che possono essere amministrative o pecuniarie e possono raggiungere i 10 milioni di euro o il 2% del fatturato mondiale annuo per i soggetti essenziali, mentre per i soggetti importanti le sanzioni sono limitate a 7 milioni di euro o l'1,4% del fatturato mondiale annuo.

Le diverse normative interagiscono e si integrano tra di loro con l'obiettivo di regolamentare il complesso mercato del cloud computing, abbiamo visto come il GDPR si concentri esclusivamente sulla regolazione dei dati personali mentre il Data Act su quelli non personali, coprendo così tutte le categorie di dati che possono far parte di un determinato dataset o elaborate tramite servizi cloud. In taluni casi quindi prevarrà il GDPR in altri il Data Act, ma la copertura offerta dall'interazione delle

due è completa. Entrambe le normative affrontano il problema della portabilità, accesso e cancellazione dei dati, il Data Act riprende questi diritti ampliandoli e adattandosi all'evoluzione tecnologica a cui stiamo assistendo, integrando per esempio dispositivi IoT e così via.

Allo stesso modo il DMA si integra con il GDPR, imponendo ai gatekeeper di garantire trasparenza e leicità nell'utilizzo dei dati raccolti, vietando pratiche come il self-preferencing che si basano sull'utilizzo improprio dei dati degli utenti. Inoltre il DMA introduce la richiesta di interoperabilità tra piattaforme e servizi, definendo regole pragmatiche per migliorare la portabilità dei dati.

Il DMA e il cybersecurity act sono complementari, infatti il primo si concentra sulla promozione della concorrenza nei mercati digitali, mentre il Cybersecurity Act mira a migliorare la sicurezza informatica.

Infine sia il Data Act che il DMA promuovono l'accesso equo ai dati, l'interoperabilità e la tutela contro l'abuso di potere, concentrandosi su player di mercato differenti.

CAPITOLO 3 – MODELLO COMPETITIVO

In questo capitolo analizzeremo tramite un modello di Hotelling le dinamiche competitive tra due cloud service providers i quali competono su prezzi e investimenti in sicurezza (modellata come un incremento delle affidabilità e quindi della qualità del servizio) a t=2 dopo aver osservato quote di mercato asimmetriche a t=1. Inoltre considereremo l'impatto degli switching costs, ovvero i costi che un cliente deve sostenere quando decide di cambiare provider rispetto al periodo precedente. Ciò può essere dovuto a diversi fattori, quali la perdita di economie di apprendimento dei dipendenti che hanno familiarizzato con il funzionamento di una determinata piattaforma cloud, ma anche le eventuali perdite nello spostamento dei dati da un fornitore all'altro, dovute alla mancanza di interoperabilità tra i diversi provider e alle commissioni d'uscita che vengono applicate.

Per la stesura del modello si è fatto riferimento ai seguenti articoli:

- "Dynamic Duopoly Competition with Switching Costs and Network Externalities" (Toker Doganoglu, Lukasz Grzybowski 2005) il quale analizza la concorrenza in un duopolio con esternalità di rete e costi di switching, ottenendo effetti opposti sulla domanda dei consumatori, mentre i primi aumentano l'elasticità della domanda, i secondi la riducono. L'articolo si concentra principalmente sul settore del software e dei sistemi operativi.
- "Connectivity in the Commercial Internet" di Jacques Crémer, Patrick Rey and Jean Tirole del 2000: gli autori considerano un duopolio di backbone (IBP) ciascuno con una propria base installata, i quali competono per attirare nuovi clienti. L'installed-base rappresenta i clienti vincolati da contratti stipulati in periodi precedenti e che pertanto non possono cambiare fornitore con facilità. Il modello assume che il beneficio che un cliente ottiene dall'adesione ad un backbone sia funzione crescente della base installata del backbone scelto, poiché sono presenti esternalità di rete, ma anche della qualità dell'interconnessione con altri backbone. L'articolo dimostra che il backbone con la base installata più grande ha incentivo a degradare la qualità dell'interconnessione con il backbone più piccolo poiché egli trae meno vantaggio da questa interconnessione.

- “A Model of Information Security and Competition” (Alexandre de Cornière e Greg Taylor, 2024), in cui gli autori mostrano come la struttura di mercato giochi un ruolo cruciale nel determinare il livello ottimo di investimenti in sicurezza, in particolare nel caso in cui gli investimenti in sicurezza creino un effetto di “business stealing” si può arrivare ad un eccessivo investimento in sicurezza da parte delle imprese rispetto al caso socialmente ottimale.

l timing del modello è il seguente:

Stadio 1: Le imprese osservano le quote di mercato

Stadio 2: Le imprese competono sia sui prezzi che sugli investimenti

La competizione si svolge in un unico periodo (t=2), durante il quale le imprese, scelgono simultaneamente il livello di investimento in sicurezza e i prezzi, internalizzando l'impatto di queste decisioni sulla domanda dei consumatori, che è funzione lineare di entrambi i fattori. Il risultato è un equilibrio di Nash statico, in cui ciascuna impresa ottimizza il proprio profitto considerando le scelte dell’altra, riflettendo così le dinamiche strategiche della competizione tra i due player.

Analizzeremo anche le scelte riguardanti gli investimenti in sicurezza, che nel contesto del cloud computing rappresentano scelte strategiche fatte dai providers per aumentare il grado di differenziazione ed evitare una guerra di prezzi.

Le funzioni di utilità del consumatore sono date dalle seguenti espressioni:

$$V_2^{aa} = u - tx + I^a - p_2^a$$

$$V_2^{bb} = u - t(1-x) + I^b - p_2^b$$

$$V_2^{ba} = u - t(1-x) + I^b - p_2^b - s^a$$

$$V_2^{ab} = u - tx + I^a - p_2^a - s^b$$

$$\pi^a = p_2^a * q_2^a - k * \frac{(I^a)^2}{2}$$

$$\pi^b = p_2^b * q_2^b - k * \frac{(I^b)^2}{2}$$

dove con V_2^{aa} ci riferiamo all'utilità che i consumatori traggono quando decidono di rimanere con il CSP^a a $t = 2$, in maniera equivalente possiamo definire V_2^{bb}.

V_2^{ab} rappresenta l'utilità dei consumatori che in t=2 decidono di cambiare provider passando dal CSP^b al CSP^ae che pertanto devono sostenere un costo di switching pari a s^b, simmetricamente per V_2^{ba}. Il parametro t rappresenta i costi di trasporto, infine k rappresenta il fattore di proporzionalità del costo marginale sostenuto dai provider. I^a e I^b rappresentano rispettivamente gli investimenti in sicurezza effettuati dal CSP^a e dal CSP^b.

3.1 ASSUNZIONI

- $s^a(x = q_1^a) < 0$: Il CSP^a ha un vantaggio perché genera "benefici" ai propri utenti;
- $0 < s^b(x = q_1^a) < 1$;
- $s^b(x = 1) > 0$;
- Il CSP^a non attua una discriminazione di prezzo tra i consumatori appartenenti alla sua installed-base e i nuovi consumatori.
- q_1^a rappresenta la quota "ereditata" dal CSP^a, è compresa nell'intervallo (0.5,1] grazie al quale possiamo definire matematicamente il vantaggio ereditato del CSP^a a t= 1
- I consumatori sono uniformemente distribuiti lungo la linea di Hotelling tra 0 e 1
- I CSP^a e CSP^b sono posizionati rispettivamente in 0 e 1
- I costi di switching sono distribuiti nell'intervallo [-1,1], data la costruzione delle funzioni di utilità del modello, i valori positivi rappresentano i costi che il consumatore deve sostenere per cambiare provider e che quindi diminuiscono la sua utilità, al contrario invece i valori negativi rappresentano dei benefici che il provider tramite il suo servizio apporta al consumatore.
- Valore massimo di $k = 5$

Dall'equazione del consumatore indifferente tra rimanere con il CSP^a oppure passare al CSP^b ricaviamo la soglia $s^a = 2tx + I^b - p_2^b + p_2^a - I^a - t$. In maniera equivalente dall'equazione

del consumatore indifferente tra rimanere con CSP^b e passare a CSP^a ricaviamo $s^b = I^a - I^b + t - 2tx - p_2^a + p_2^b$.

Per la risoluzione del modello, il primo passo è calcolare la domanda per i CSP^i a $t = 2$

Per calcolare la domanda per il CSP^a sommiamo ai consumatori dell'installed-base del provider a, anche tutta la quota di mercato che riesce a sottrarre al provider b, ovvero l'area sottesa ad s^a. Pertanto la domanda totale per il CSP^a sarà pari a:

$$q_2^a = q_1^a * 1 + [s^b(x = q_1^a) + s^b(x = 1)] * \frac{(1 - q_1^a)}{2}$$

La quota di consumatori del CSP^b invece sarà data da tutti quei consumatori che hanno un costo di switching superiore alla soglia s^b data la loro posizione lungo la linea di Hotelling, pertanto essa sarò pari a:

$$q_2^b = \left[\left(1 - s^b(x = 1)\right) + \left(1 - s^b(x = q_1^a)\right)\right] * \frac{(1 - q_1^a)}{2}$$

Partendo da questa espressione e sostituendovi

$$s^b(x = 1) = I^a - I^b - t - p_2^a + p_2^b.$$

$$s^a(x = q_1^a) = 2tq_1^a + I^b - p_2^b + p_2^a - I^a - t$$

$$s^b(x = q_1^a) = I^a - I^b + t - 2tq_1^a - p_2^a + p_2^b.$$

otteniamo q_2^a e q_2^b in funzione di I^a, I^b p_2^a, p_2^b, t e q_1^a

$$q_2^a = q_1^a + (q_1^a - 1)(-I^a + I^b + p_2^a - p_2^b + tq_1^a)$$

$$q_2^b = (1 - q_1^a)(1 - I^a + I^b + p_2^a - p_2^b + tq_1^a)$$

Avendo ricavato le quantità di equilibrio a t=2 possiamo procedere con la massimizzazione delle due funzioni di profitto rispetto a p_2^a e p_2^b

L'espressione delle funzioni di profitto sarà:

$$\pi^a = [q_1^a + (q_1^a - 1)(-I^a + I^b + p_2^a - p_2^b + tq_1^a]^* p_2^a - k * \frac{(I^a)^2}{2}$$

$$\pi^b = [(1 - q_1^a)(1 - I^a + I^b + p_2^a - p_2^b + tq_1^a)]^* p_2^a - k * \frac{(I^a)^2}{2}$$

Procediamo quindi con la massimizzazione del profitto π^a e π^b rispetto a p_2^a e p_2^b

$$\begin{cases} \dfrac{\partial \pi^a}{\partial p_2^a} = q_1^a + (I^a - I^b + p_2^b - \mathrm{t}q_1^a)(1 - q_1^a) - 2p_2^a(1 - q_1^a) \\ \dfrac{\partial \pi^b}{\partial p_2^b} = (1 - I^a + I^b + p_2^a + tq_1^a)(1 - q_1^a) - 2p_2^a(1 - q_1^a) = 0 \end{cases}$$

Otteniamo $p_2^{*a}(I^a, I^b)$ e $p_2^{*b}(I^a, I^b)$,

$$p_2^{*a} = \frac{1}{3}\left(-1 + I^a - I^b - \frac{2}{q_1^a - 1} - tq_1^a\right)$$

$$p_2^{*a} = \frac{1}{3}\left(1 - I^a + I^b + \frac{1}{1 - q_1^a} + tq_1^a\right)$$

Avendo ottenuto p_2^{*a} e p_2^{*b} possiamo sostituirli nelle funzioni di profitto, cosicché adesso siano funzione solamente di I^a, I^b, k, q_1^a.

Procediamo derivando nuovamente le funzioni di profitto rispetto agli investimenti così da ricavare la quantità ottima di equilibrio di entrambi i provider.

$$\begin{cases} \frac{\partial \pi^a}{\partial I^a} = \frac{1}{9}(I^a(2 - 9k - 2q_1^a) + 2\left(1 + q_1^a + (q_1^a - 1)(I^b + tq_1^a)\right) = 0 \\ \frac{\partial \pi^b}{\partial I^b} = -I^b k - \frac{2}{9}\left(-2 + I^a + q_1^a - I^a q_1^a + (q_1^a - 1)(I^b + tq_1^a)\right) = 0 \end{cases}$$

Da cui ricaviamo

$$I^{*a} = \frac{-4 + 6k(1 + q_1^a)}{3k(9k - 4)};$$

$$I^{*b} = \frac{4 + 6k(-2 + q_1^a)}{3k(4 - 9k)};$$

$$p_2^{*a}(k, q_1^a) = q_2^{*a}(k, q_1^a) = \frac{-2 + 3k(1 + q_1^a)}{9k - 4};$$

$$p_2^{*b}(k, q_1^a) = q_2^{*b}(k, q_1^a) = \frac{2 + 3k(q_1^a - 2)}{4 - 9k};$$

ed infine

$$\pi^{*a}(k, q_1^a) = \frac{(9k - 2)[2 - 3k(1 + q_1^a)]^2}{9k(4 - 9k)^2}$$

$$\pi^{*b}(k, q_1^a) = \frac{(9k - 2)[2 + 3k(q_1^a - 2)]^2}{9k(4 - 9k)^2}$$

Imponendo la condizione che profitti, prezzi (e quindi quantità) e investimenti siano positivi e che siano rispettate le ipotesi sulle soglie s^b e s^a troviamo che:

$$k \in \left(-\frac{2}{3q_1^a-6}; \frac{2}{3}\right) \; e \; t \in \left(0; \frac{(3k-2)(1-2q_1^a)}{9k-4}\right)$$

3.2 EQUILIBRIO AL VARIARE DELLA BASE INSTALLATA q_1^a

Iniziamo con l'analizzare la quota di mercato dei due CSP^i

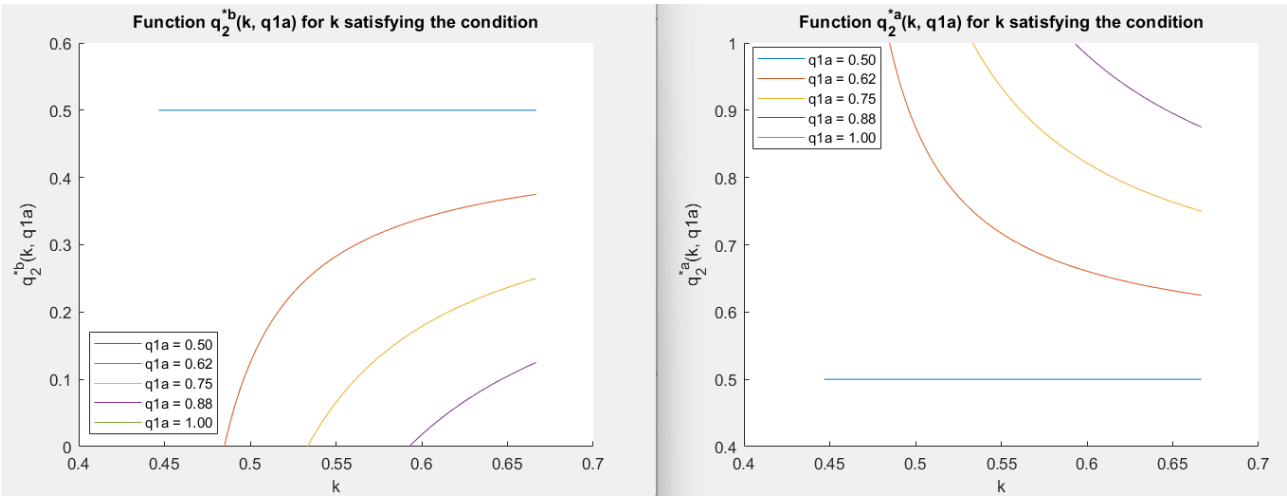

Figure 11: Andamento delle quote di mercato di equilibrio dei due CSP al variare dei parametri k e q1a

Le due quote di mercato, come mostrato dai grafici sopra, evidenziano la relazione complementare che sussiste tra i due provider, nel caso in cui $q_1^a = 0.5$ entrambi i provider coprono esattamente metà mercato, questa rappresenta la situazione di perfetta simmetria in cui nessuno prevale sull'altro. Man mano che il vantaggio del CSP^a cresce, ci allontaniamo sempre di più da questa situazione simmetrica, infatti la quota di mercato del provider a crescerà sempre di più all'aumentare di q_1^a, costringendo il provider b a ridurre la suo quota di mercato, fino al caso limite in cui $q_1^a = 1$ e il provider b, non ha nessuna possibilità di accedere al mercato che risulta dominato interamente dal provider a. Dai grafici vediamo chiaramente come $q_1^a = 0.5$ rappresenti il lower bound per CSP^a e l'upper bound della quota di mercato per CSP^b.

Proseguiamo con lo studio delle scelte di investimento

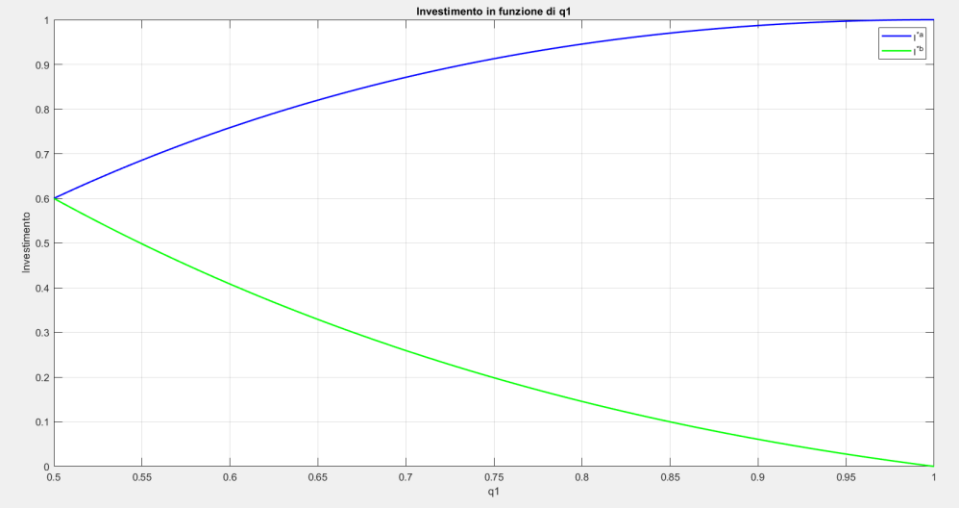

Figure 12: Confronto tra le scelte dei livelli di investimento di equilibrio dei due CSP al variare di q1a

Come possiamo vedere, le scelte sui livelli di investimento dei due provider sono divergenti. Il provider a è incentivato ad investire sempre di più al crescere della sua installed-base e per valori di k inferiori, ovvero quando il costo dell'investimento è particolarmente basso. La risposta ottima del provider b, invece è quella di investire sempre meno all'aumentare di q_1^a , poiché il suo livello di investimento sarebbe di molto inferiore rispetto a quello del provider a, per cui non riuscirebbe a trattenere nessuno dei suoi clienti, fino al caso limite in cui analizzare il livello di investimenti perde di significato in quanto tutto il mercato è coperto dal provider a.

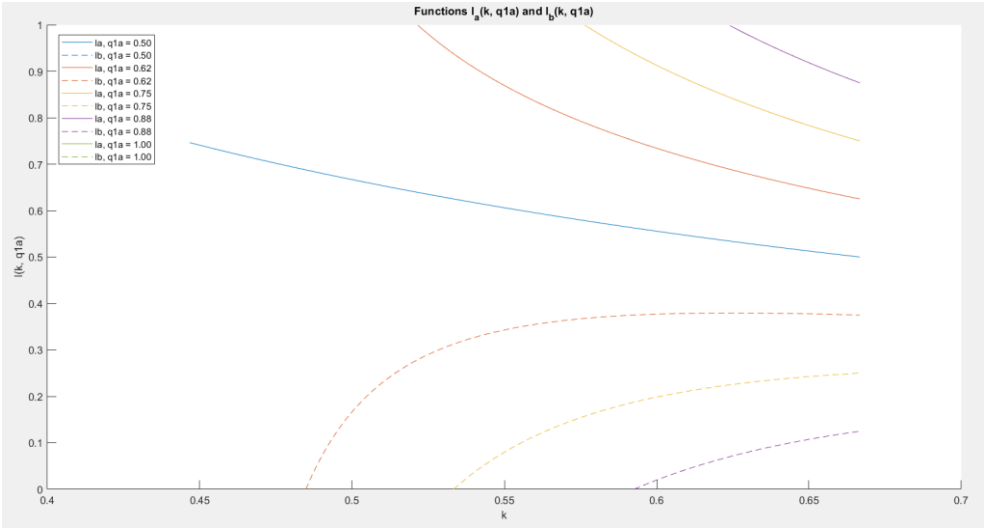

Figure 13: Confronto tra le funzioni di investimento di equilibrio dei CSP al variare di k e q1a

All’aumentare di k, la forbice tra i due livelli di investimento si restringe, poiché investire risulta più costoso pertanto il provider a riduce il suo livello di investimento.

Questo crea spazio per il provider b, che inizia ad investire (ovviamente, nel caso in cui i valori di q_1^a non siano troppo elevati) così da riuscire a mantenere una quota dei suoi consumatori, offrendo un servizio con una qualità superiore, ed evitando che tutti passino al provider a. Questo porta ad una conseguenza poco intuitiva, ovvero *l’impresa b investa di più all’aumentare di k* (coefficiente di proporzionalità del costo marginale degli investimenti in sicurezza.

Proseguendo l’analisi con lo studio delle funzioni di profitto dei due provider vediamo come il CSP^a realizzi sempre un profitto superiore rispetto al suo concorrente. Il suo profitto cresce al crescere della installed-base e diminuisce all’aumentare di k, perché il CSP^a decide di investire meno e quindi la sua quota di mercato diminuisce all’aumentare di k. In modo complementare invece il profitto del suo concorrente aumenta con k, perché per valori più alti di k, inizia ad investire in sicurezza e questo gli permette di mantenere parte della suo quota iniziale di mercato.

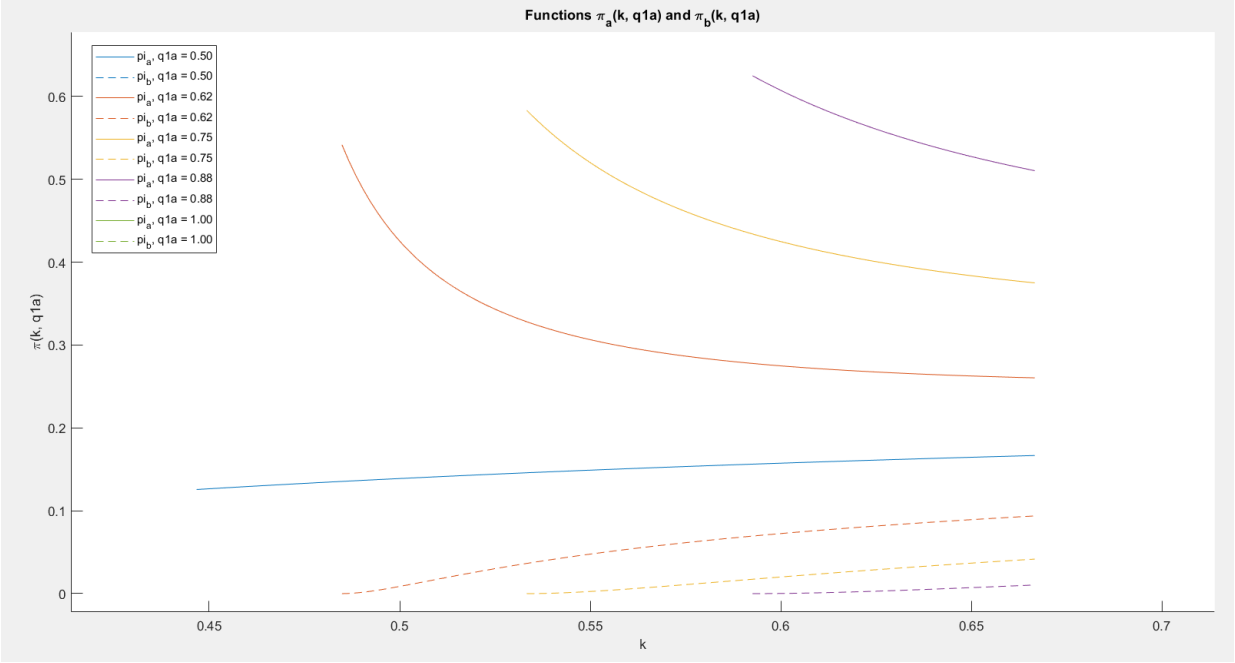

Figura 14: confronto tra le funzioni di profitto di equilibrio dei due CSP al variare di k e q1a

Dall'equazione del consumatore indifferente a t=2 tra rimanere con il CSP^a oppure passare al provider b, ricaviamo la soglia dei costi di switching.

$$s^a(x, q_1^a, k, t) = \frac{2 + t(4 - 8x) - 4q_1^a + 3k(-1 + t(-3 + 6x) + 2q_1^a)}{-4 + 9k}$$

Allo stesso modo possiamo ricavare s^b dall'equazione del consumatore indifferente tra rimanere con il provider b oppure passare al provider a:

$$s^b(x, q_1^a, k, t) = \frac{-2 + t(-4 + 8x) + k(3 + t(9 - 18x) - 6q_1^a) + 4q_1^a}{-4 + 9k}$$

Queste funzioni rappresentano in ogni punto il costo (o il beneficio, per valori negativi) che i clienti devono pagare (o ricevono) per passare (rimanere) all'altro provider. Entrambe variano, in modo diverso, con t, k, x (ovvero la posizione del generico consumatore lungo la linea di Hotelling) e q_1^a.

Procediamo con l'analisi della soglia di switching del CSP^a calcolata in q_1^a che per ipotesi abbiamo assunto essere sempre negativa.

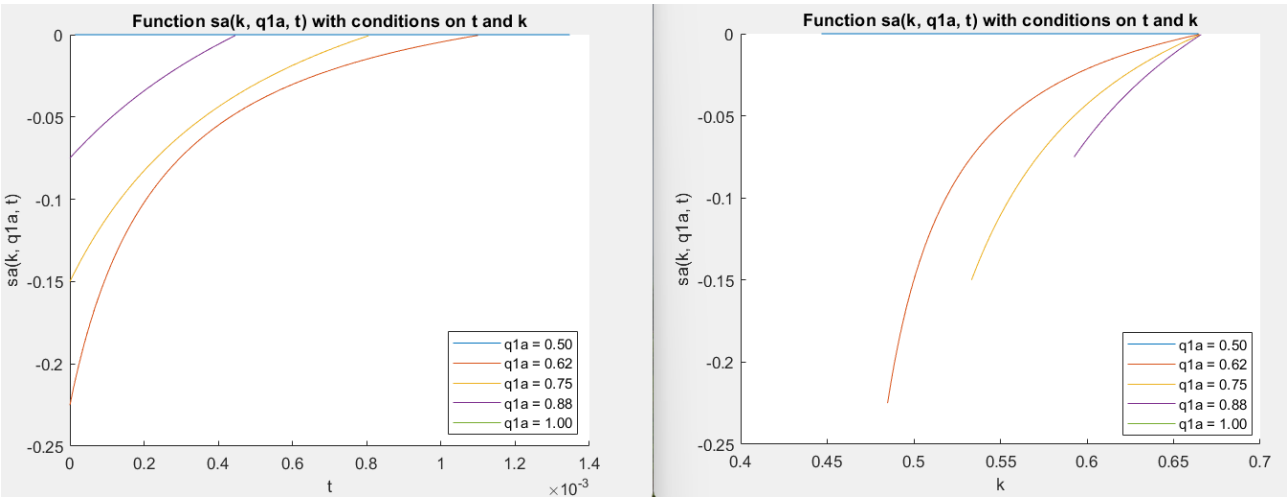

Figure 15: Andamento della soglia di switching del CSP^a.

Studiamo $|s^a|$ al variare dei parametri: k, t e q_1^a.

- Risulta crescente con k (coefficiente di proporzionalità del costo marginale), questo perché, come abbiamo visto gli investimenti in sicurezza del CSP^a sono decrescenti con k, ciò diminuisce l'utilità del consumatore che a t=1 aveva scelto questo provider, pertanto aumenta la probabilità che decida di cambiare e passare al CSP^b
- E' positivamente correlata con t, $\frac{\partial s^a}{\partial t} \geq 0$, poiché il CSP^a parte con un vantaggio che gli permette di catturare consumatori abbastanza "lontani" da zero, pertanto all'aumentare del costo di trasporto, diminuisce la probabilità che rimangano con il CSP^a
- Infine risulta crescente anche con q_1^a. Ragionando similmente al caso del costo di trasporto possiamo intuire come al crescere di q_1^a , i consumatori siano sempre più distanti dal CSP^a pertanto risulta perfettamente ragionevole pensare che siano indotti a passare con il CSP^b in quanto risulta più "vicino" alle loro preferenze.
- s^a risulta crescente sia al crescere di I^b che di p_2^a, ovvero più sono alti gli investimenti in sicurezza del CSP^b più la soglia di switching si alza (cioè più consumatori passano dal CSP^a al CSP^b, ciò risulta perfettamente sensato visto che gli investimenti in sicurezza rappresentano un fattore differenziante, indice di qualità del provider. Ovviamente ci aspettiamo che più p_2^a sia alto più i clienti siano incentivati a spostarsi verso l'altro provider.
- s^a risulta decrescente sia al crescere di I^a che di p_2^b e s^b risulta decrescente sia al crescere di I^b che di p_2^a.

Passiamo adesso allo studio della s^b, per ipotesi abbiamo imposto che essa debba essere positiva lungo il tratto $1 - q_1^a$ della linea di Hotelling, infatti dai grafici possiamo subito notare che non raggiunge mai valori negativi, il lower bound è rappresentato dal caso $q_1^a = 0.5$ in cui entrambi i provider soddisfano metà domanda e nessuno dei consumatori del CSP^b passa al CSP^a e viceversa.

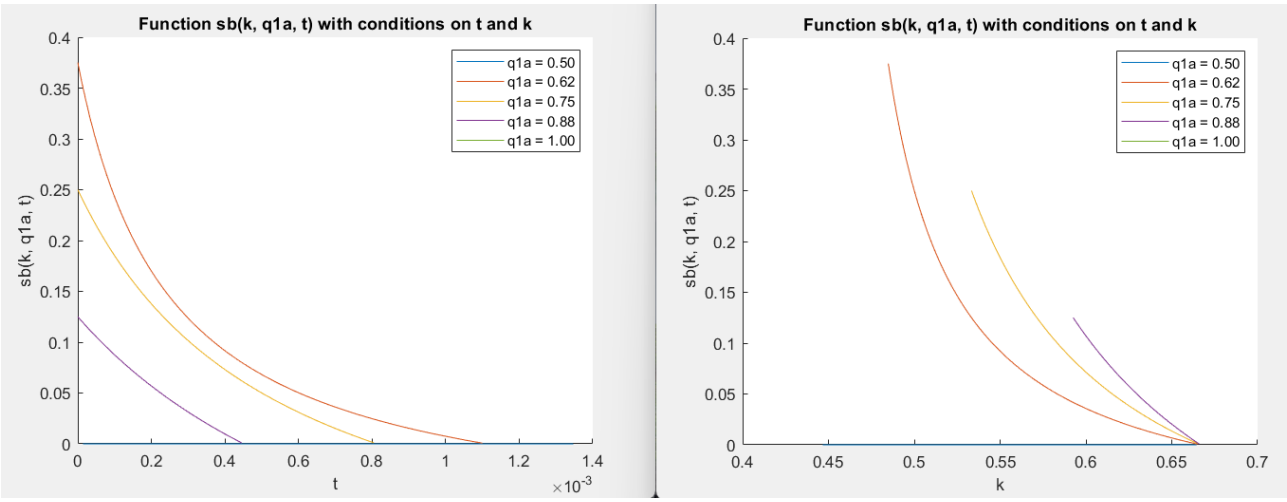

Figure 16: Andamento della soglia di switching del CSP^b.

- La funzione decresce al crescere di k. Come abbiamo visto gli investimenti in sicurezza del CSP^b aumentano con k, ciò impatta positivamente sull'utilità dei consumatori che pertanto saranno più invogliati a rimanere con il CSP^b.
- La soglia s^b, $\frac{\partial s^b}{\partial t} \leq 0$, è decrescente anche con il costo di trasporto t, in accordo con quanto detto sulla relazione tra s^a e t e la complementarietà tra q_2^a e q_2^b, possiamo subito capire che tutti i clienti che il provider a perderà all'aumentare del costo di trasporto, saranno conquistati dal provider b.
- s^b risulta crescente sia al crescere di I^a che di p_2^b, ovvero più sono alti gli investimenti in sicurezza del CSP^a più la soglia di switching si alza (cioè più consumatori passano dal CSP^b al CSP^a, come avevamo già visto per il provider a. Ovviamente ci aspettiamo che più p_2^b sia alto più i clienti siano incentivati a spostarsi verso l'altro provider.
- Infine decresce anche con q_1^a, poiché più il consumatore è posizionato vicino al provider b, più è probabile che decida di servirsi da lui.

Infine sia s^a che s^b risultano funzione di x, ovvero della generica posizione del consumatore lungo la linea di Hotelling, in particolare s^a risulta crescente in x $\left(\frac{\partial s^a}{\partial x} > 0\right)$, invece s^b è decrescente all'aumentare di x $\left(\frac{\partial s^b}{\partial x} < 0\right)$.

Pertanto abbiamo dimostrato come il CSP^a grazie al suo vantaggio iniziale e agli switching costs riesca non soltanto a mantenere il suo vantaggio ma a cumularlo nel tempo, strappando consumatori al CSP^b. Inoltre gli switching costs gli permettono di investire di più in sicurezza aumentando così la qualità del suo servizio e rendendolo così più attrattivo agli occhi dei clienti.

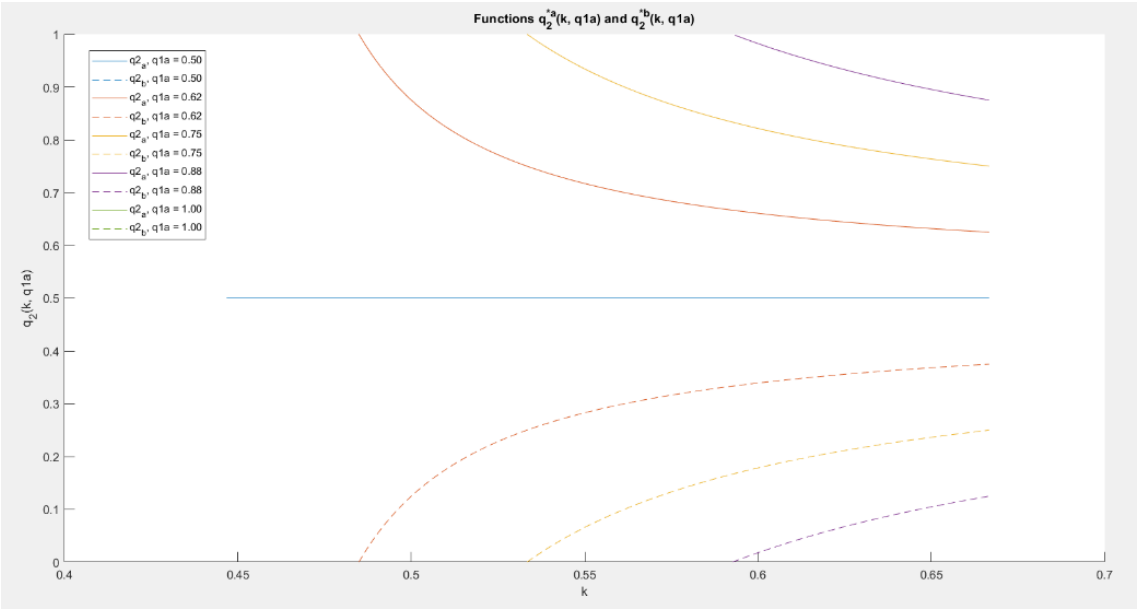

Figure 17: Confronto tra le quote di mercato di equilibrio dei CSP

CONCLUSIONE

Abbiamo ripercorso la storia del cloud dagli albori fino ad oggi osservando come negli ultimi due decenni abbia trasformato profondamente la competizione in tutti i settori, dall'industriale, passando per il finanziario fino al settore medicale. Nonostante il cloud abbia rappresentato un motore d'innovazione straordinario permettendo ad organizzazioni di ogni dimensione di competere su scala globale, oggi stanno riaffiorando problematiche legate ai costi e alla dipendenza strategica. Questo è dovuto alla struttura stessa del mercato del cloud computing, il quale è caratterizzato da forti economie di scala dei provider (non a caso denominati hyperscalers), switching cost e mancanza di interoperabilità, tutti fattori che impediscono il multihoming e portano ad un'elevata concentrazione di mercato con un HHI>3.

Nel lavoro di tesi dimostro come, la presenza degli switching costs contestualmente ad una installed-base ed investimenti in sicurezza, utilizzati strategicamente per aumentare l'utilità dei consumatori e la differenziazione, portino ad una ulteriore consolidazione della posizione dominante del provider, estromettendo dal mercato i CSP di dimensioni inferiori, i quali non riescono a raggiungere i livelli di investimenti in sicurezza degli hyperscalers. Di conseguenza i clienti tenderanno sempre a scegliere il provider che investe maggiormente in sicurezza, vista la rilevanza della cybersecurity nell'ambito del cloud computing, giungendo ad una struttura di mercato oligopolistica, nella quale non viene massimizzato il benessere collettivo, ma bensì quello delle imprese che la governano. Infatti i prezzi imposti dagli attori dominanti sono sempre superiori rispetto a quelli del CSP con una quota inferiore.

Pertanto se fino ad ora, proprio per il ruolo cruciale del cloud nell'economia digitale, è stato difficile per i legislatori sviluppare normative capaci di contenere il potere crescente dei grandi provider senza compromettere la spinta innovativa e lo sviluppo economico che ne derivano, ad oggi considerando anche l'avvento dell'intelligenza artificiale e della richiesta di spazio di elaborazione, non ci sono più dubbi sulla necessità di un intervento normativo stringente che elimini l'abuso di posizione dominante. A tal proposito risulta incoraggiante l'intervento Europeo con il Data Act, le cui disposizioni saranno pienamente applicabili nel 2025, nel quale si punta a creare un ecosistema armonizzato ed equo all'interno dell'Unione.

Bibliografia

1. **Completamento della migrazione su cloud di Netflix, 2016** https://about.netflix.com/it/news/completing-the-netflix-cloud-migration
2. **PaaS, IaaS, SaaS e CaaS: in che cosa differiscono?** Google Cloud, https://cloud.google.com/learn/paas-vs-iaas-vs-saas?hl=it
3. **What is SaaS?** Microsoft, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-saas
4. **Che cos'è l'architettura cloud?** Pavel Despot, 2023, https://about.netflix.com/it/news/completing-the-netflix-cloud-migration
5. **Definizione e confronto tra i vari tipi di cloud,** https://www.redhat.com/it/topics/cloudcomputing/public-cloud-vs-private-cloud-and-hybrid-cloud
6. **IPCEI sulle infrastrutture e i servizi cloud di prossima generazione per promuovere il decennio digitale europeo,** Commissione Europea, 2023. https://digital-strategy.ec.europa.eu/it/news/ipcei-next-generation-cloud-infrastructure-and-services-boost-europes-digital-decade
7. **I vantaggi dell'edge computing,** Red Hat, 2021 https://www.redhat.com/it/topics/edge-computing/what-is-edge-computing
8. **Edge Computing e sicurezza, quali le sfide che le aziende si trovano ad affrontare**, Rodolfo Falcone, 2023 https://www.cybersecurity360.it/soluzioni-aziendali/edge-computing-e-sicurezza-quali-le-sfide-che-le-aziende-si-trovano-ad-affrontare/
9. **Decisione UE 2022/2481,** https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32022D2481
10. **Direttiva UE 2022/2555,** https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32022L2555
11. **Il potenziale dell'Europea nell'Edge Computing: Sostenere l'innovazione industriale attraverso progetti pilota su larga scala,** Commissione Europea, 2023

https://digital-strategy.ec.europa.eu/it/library/europes-potential-edge-computing-supporting-industrial-innovation-through-large-scale-pilots

12. **Study on the Economic Potential of Far Edge Computing in the Future Smart Internet of Things, European Union, 2023** https://op.europa.eu/en/publication-detail/-/publication/ff35c457-8f3b-11ee-8aa6-01aa75ed71a1
13. **Gartner Magic Quadrant for Strategic Cloud Platform Services 2023,** CX Today 2024, https://www.cxtoday.com/data-analytics/gartner-magic-quadrant-for-strategic-cloud-platform-services-2023/
14. **AWS, Microsoft, Google, Oracle lead in Gartner's Magic Quadrant for Strategic Cloud Platform Services,** DHN Weekly Tech Updates, 2024, https://www.linkedin.com/pulse/aws-microsoft-google-oracle-lead-gartners-magic-quadrant-obavc/
15. **Il magic quadrant di gartner per l'e-commerce** http://www.ecommerceelogistica.it/magic-quadrant-gartner-per-ecommerce/
16. **Amazon Web Services (AWS): vantaggi, casi d'uso e applicazioni,** Claranet 2022**,** https://www.claranet.com/it/blog/amazon-web-services-vantaggi-applicazioni#vantaggi-cloud-computing-AWS
17. **Magic Quadrant for Strategic Cloud Platform Services,** David Wright and Dennis Smith, 2023 https://www.gartner.com/doc/reprints?id=1-2FTDYPQN&ct=231204&st=sb
18. **Cloud computing, quali sono i principali player del mercato,** Giovanni Sisinna, 2022 https://www.bigdata4innovation.it/big-data/cloud-computing/cloud-computing-quali-sono-i-principali-player/
19. **Microsoft and Amazon Dominate the Cloud,** Martin Armstrong https://www.statista.com/chart/30489/revenue-from-cloud-services-by-cloud-sector-market-leaders/
20. **Alibaba Cloud Computing: An Introduction,** NetApp BlueXP, 2018 https://bluexp.netapp.com/blog/alibaba-cloud-computing-an-introduction
21. **Alibaba forms Cloud Intelligence Group as separate business,** Georgia Butler 2023 https://www.datacenterdynamics.com/en/news/alibaba-forms-cloud-intelligence-group-as-separate-business/

22. **IBM Cloud: cos'è e come usarlo per sviluppare intelligenza artificiale in azienda,** ZeroUno 2020**,** https://www.zerounoweb.it/resource-center/data-science-machine-learning/ibm-cloud-cose-e-come-usarlo-per-sviluppare-intelligenza-artificiale-in-azienda/
23. **What is the IBM Cloud platform?** IBM Cloud 2024, https://cloud.ibm.com/docs/overview?topic=overview-whatis-platform
24. **Il cloud computing nel 2024 e i 10 principali fornitori di servizi cloud,** Filip Stojanovic, https://tridenstechnology.com/it/fornitori-di-servizi-cloud/
25. **Google complains to EU over Microsoft cloud practices**, Philip Blenkinsop, 2024 https://www.reuters.com/technology/google-files-complaint-eu-over-microsoft-cloud-practices-2024-09-25/
26. **Harm of Giants in Cloud computing Market,** Kure Chel Lee, Yun Ho Choi, Ki Duck Kim, 2023
27. **The World Will Store 200 Zettabytes of Data By 2025,** Cybersecurity Ventures, 2024, https://cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/
28. **Cos'è la Cybersecurity e perché è importante in azienda**, Osservatorio Cybersecurity & Data Protection, https://blog.osservatori.net/it_it/cose-cyber-security-significato-principi-tecnologie
29. **AI Power: Expanding data center capacity to meet growing demand,** McKinsey & Company, 2024 https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/ai-power-expanding-data-center-capacity-to-meet-growing-demand
30. **Cloud Security 101: Challenges and Best Practices,** Scrut Automation, 2023
31. **Cos'è DevSecOps,** AWS, https://aws.amazon.com/it/what-is/devsecops/#:~:text=DevSecOps%20%C3%A8%20sinonimo%20di%20sviluppo,la%20creazione%20di%20applicazioni%20software
32. **L'impatto del cyber risk sul mercato finanziario**, GCSEC, 2020
33. **Disaster Recovery: cos'è e perchè e fondamentale per le aziende,** ACS, 2023 https://www.acs.it/it/blog/digitalizzazione-aziendale/disaster-recovery-cos-e/
34. **Regolamento UE 2016/679,** https://eur-lex.europa.eu/legalcontent/IT/TXT/?uri=celex%3A32016R0679
35. **Regolamento UE 2023/2854**, https://eur-lex.europa.eu/eli/reg/2023/2854/oj

36. **Competition and regulation of cloud computing services: economic analysis and review of eu policies.** CERRE report, February 2024
37. **Data Act: guida alle nuove regole per l'accesso e l'uso dei dati in Europa,** Network Digital 360, 2024 https://www.agendadigitale.eu/mercati-digitali/data-act-guida-alle-nuove-regole-per-laccesso-e-luso-dei-dati-in-europa/
38. **Cloud computing e GDPR: regole di accountability per il trasferimento dei dati all'estero,** Andrea Afferni, 2019, https://www.cybersecurity360.it/legal/privacy-dati-personali/cloud-computing-e-gdpr-regole-di-accountability-per-il-trasferimento-dei-dati-allestero/
39. **Microsoft supports new rules for gatekeepers,** Microsoft 2021, https://blogs.microsoft.com/eupolicy/2021/05/03/microsoft-supports-new-rules-for-gatekeepers/
40. **DMA, nuove regole per app, gatekeeper e interoperabilità: cosa cambia nel testo finale**, Nadia Giusti, 2022, https://www.cybersecurity360.it/legal/privacy-dati-personali/dma-nuove-regole-per-app-gatekeeper-e-interoperabilita-cosa-cambia-nel-testo-finale/
41. **Digital markets act, paradossa cloud: le Big tech resteranno 'senza regole'?,** Patrizia Licata, 2021 https://www.corrierecomunicazioni.it/digital-economy/cloud/digital-markets-act-paradosso-cloud-le-big-tech-resteranno-senza-regole/
42. **REGOLAMENTO (UE) 2022/1925**, https://eurlex.europa.eu/legalcontent/IT/TXT/?uri=celex:32022R1925
43. **In che modo il Digital Markets Act (DMA) Europeo influisce sulla privacy degli utenti e sulla gestione del consenso,** Usercentrics, 2023, https://usercentrics.com/it/knowledge-hub/digital-market-act
44. **Regolamento UE 2019/881,** https://eur-lex.europa.eu/eli/reg/2019/881/oj?locale=it
45. **Le nuove certificazioni cloud europee: cosa sono e perché preoccupano le big tech,** Davide Agnello, 2022**,** https://www.agendadigitale.eu/sicurezza/le-nuove-certificazioni-cloud-europee-cosa-sono-e-perche-preoccupano-le-big-tech/
46. **Nis2, come adeguarsi ai nuovi obblighi cyber:** i punti chiave, Gabriele Faggioli, 2024**,**

https://www.agendadigitale.eu/sicurezza/obblighi-di-cyber-sicurezza-come-adeguarsi-alla-direttiva-nis2/

47. **Direttiva NIS 2, gli impatti sulle aziende: cosa fare per adeguarsi**, Marco Gentilini, 2023, https://www.cybersecurity360.it/cybersecurity-nazionale/direttiva-nis-2-gli-impatti-sulle-aziende-cosa-fare-per-adeguarsi/

48. **Regolamento generale per la protezione dei dati,** Bruno Saetta, 2023, https://protezionedatipersonali.it/regolamento-generale-protezione-dati

49. Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing: https://www.etsi.org/deliver/etsi_sr/003300_003399/003391/02.01.01_60/sr_003391v020101p.pdf

50. **"Dynamic Duopoly Competition with Switching Costs and Network Externalities",** Toker Doganoglu, Lukasz Grzybowski, 2005

51. **Connectivity in the Commercial Internet"**, Jacques Crémer, Patrick Rey and Jean Tirole,2000

52. A Model of Information Security and Competition, Alexandre de Cornière e Greg Taylor, 2024